Как не стать жертвой киберпреступлений

Достижения науки и техники, создание всемирной сети интернет позволили преступности выйти на новый уровень и захватить киберпространство.

Теперь преступнику не нужен прямой контакт с жертвой, он может стать угрозой для каждого пользователя «глобальной паутины», крупных корпораций и целых государств.

Преступность в виртуальном пространстве – явление относительно новое, но часть преступлений, совершаемых в сфере высоких технологий, – это знакомые кражи, мошенничества, вымогательство.

Киберпреступность – незаконные действия, которые осуществляются людьми, использующими информационные технологии для преступных целей. Среди основных видов киберпреступности выделяют распространение вредоносных программ, взлом паролей, кражу номеров кредитных карт и других банковских реквизитов, а также распространение противоправной информации с использованием сети Интернет.

Правила, которые помогут Вам не стать жертвой киберпреступлений:

- храните номер карточки и ПИН–коды в тайне;

- не используйте один пароль для всех интернет-ресурсов;

- к своей основной карте в Вашем банке выпустите дополнительную, которой будете расплачиваться в интернете. Туда легко можно будет переводить небольшие суммы денег, и в случае компрометации данных достаточно просто заблокировать ее;

- регулярно проверяйте состояние своих банковских счетов, чтобы убедиться в отсутствии «лишних» и странных операций;

- поставьте лимит на сумму списаний или перевода в личном кабинете банка;

- не перечисляйте деньги на электронные кошельки и счета мобильных телефонов при оплате покупок, если Вы не убедились в благонадежности лица/организации, которым предназначаются Ваши средства;

- не переводите денежные средства на счета незнакомых лиц;

- не перезванивайте и не направляйте ответные SMS, если Вам поступило сообщение о блокировании банковской карты. Свяжитесь с банком, обслуживающим Вашу карту;

- будьте осмотрительны в отношении писем с вложенными картинками, поскольку файлы могут содержать вирусы. Открывайте вложения только от известных Вам отправителей и всегда проверяйте вложения на наличие вирусов, если это возможно;

- не переходите необдуманно по ссылкам, содержащимся в спам-рассылках. Удостоверьтесь в правильности ссылки, прежде чем переходить по ней из электронного письма;

- не заполняйте полученные по электронной почте формы и анкеты. Личные данные безопасно вводить только на защищенных сайтах;

- насторожитесь, если от Вас требуют немедленных действий или представляется чрезвычайная ситуация. Это тоже может быть мошенничеством, преступники вызывают у Вас ощущение тревоги, чтобы заставить Вас действовать быстро и неосмотрительно;

- не размещайте в открытом доступе и не передавайте информацию личного характера.

Рассмотрим самые распространенные схемы мошенничества:

1. **«Звонок из Банка»**

Вам звонит незнакомец. Номер входящего звонка очень похож на номер банка, а звонящий представляется работником контакт-центра или службы безопасности банка.

Для реализации мошеннической схемы также используются мессенджеры, прежде всего Viber. Входящий звонок максимально закамуфлирован под звонок сотрудника банка: на аватарке может использоваться логотип банка (полностью или частично), а отображаемый телефонный номер звонящего может быть очень похож на телефон службы поддержки банка.

У мошенников есть возможность звонить с номеров, похожих на официальные номера банка. Злоумышленники меняют цифры в номере, которые вы можете не заметить.

У вас просят конфиденциальные данные

Мошенник сообщает, что «банк выявил подозрительную операцию по Вашей карте» или «поступил запрос на онлайн-оформление кредита на Ваше имя».

Он просит у вас логин и пароль от Интернет-банкинга, код из SMS от Банка (в большинстве случаев сопровождаемый фразой «Никому не сообщайте!»), реквизиты карты (полный номер карты и срок ее действия, CVV- или CVC-код). Это нужно якобы «для сохранности ваших денег».

Как мошенник пытается вас убедить

- «*Мы звоним с официального номера, проверьте на сайте».*
- *«В целях конфиденциальности я включаю робота, который защитит ваши данные»* (вы слышите в трубке лёгкий шелест).
- Для убедительности он называет ваши персональные данные (имя, отчество, последние 4 цифры карты и др.) и просит перевести деньги *«на защищённый счет, который закреплён за персональным менеджером: это нужно для безопасности, а потом вы сможете вернуть деньги».*
- Или просит назвать ваши персональные данные или секретные коды из SMS роботу, при этом в трубке вы слышите музыку.
- Вам предлагают услуги страховки от мошеннических действий. Для ее оформления необходимо предоставить данные о карте, на которой находятся значительные денежные средства и SMS-код для подтверждения операции.

Важно! Никому не сообщайте свои личные данные, данные карт, защитные коды, коды из SMS! Если с картой, действительно, происходят мошеннические операции, Банк сам может ее заблокировать!

2. **«Потенциальный покупатель»**

Мошенник представляется потенциальным покупателем товара, объявление о продаже которого было размещено вами в сети интернет. По каким-то причинам «покупатель» не может сегодня привезти деньги, но хочет прислать вам залог из другого города по системе дистанционного банковского обслуживания.

Ссылка

Для проверки поступления перевода мошенник направляет вам ссылку на фишинговый сайт, который очень близок по дизайну на используемый вами интернет-банк или страницу для ввода реквизитов карточки для получения уже отправленного перевода денежных средств. После введения вами в поля фишингового сайта пароля и логина или реквизитов вашей карточки, данные становятся доступны мошеннику.

QR-код

Вместо ссылки мошенник может направить вам QR-код, который также хранит в себе ссылку на фишинговый сайт. После введения вами в поля фишингового сайта пароля и логина или реквизитов вашей карточки, данные становятся доступны мошеннику.

Важно! Не переходите по подозрительным ссылкам. Для веб-версии Интернет-банкинга используйте только официальный сайт Банка, а для мобильной версии – только мобильное приложение, загруженное из официальных магазинов. Внимательно изучите сайт, на котором вводите личные данные. Обязательно проверьте наличие такого сайта в интернете.

Запомните! Для получения перевода денежных средств нет необходимости вводить срок действия карты и CVV-код.

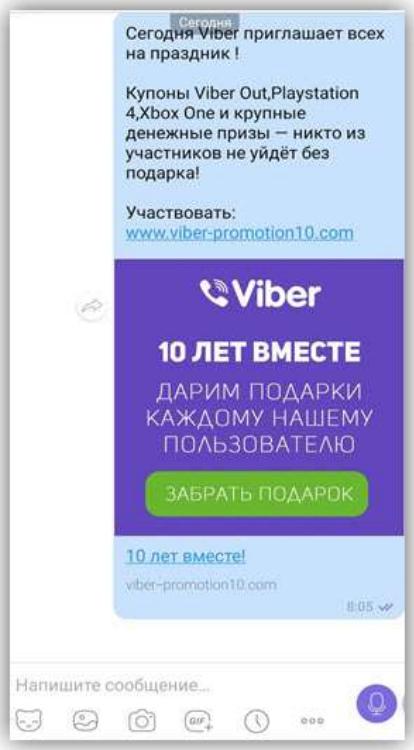
3. **«Сообщения в социальных сетях»**

Мошенник незаконным путем получает доступ к страничке в социальной сети и отправляет сообщения с просьбой финансовой помощи от имени ее владельца друзьям.

Просьба может быть самая разная: от «Скинь мне денег на карту, по дружбе» до нехватки денег на большую покупку. В редких случаях мошенник даже просит произвести оплату самостоятельно, обещая возместить затраты при личной встрече.

Важно! При получении сомнительного сообщения или малейшей неуверенности в том, что вы действительно общаетесь с владельцем странички, позвоните ему.

4. **«Розыгрыши/раздачи/опросы от Банка или иных организаций»**



Мошенники оставляют выдуманную рекламу в популярных социальных сетях об опросе от имени Банка и «Раздаче призов первой 1000 прошедших опрос!» или о том, что в связи я годовщиной Банка либо иным значимым мероприятием, последний раздает своим клиентам денежные призы. Цель опроса — якобы изучить мнение клиентов. После прохождения опроса организатор обещает денежное вознаграждение.

Однако, после прохождения опроса необходимо заплатить небольшую комиссию, связанную с перечислением вознаграждения либо с целью получения последнего – ввести данные Вашей банковской карты.

Данный кейс очень разнообразен и ограничивается только воображением мошенников. Вместо опроса может предлагаться возмещение налоговых выплат, компенсация за наличие ваших данных в базе «утечки» и иные махинации.

Важно! Посетите официальную страницу организации или позвоните в контакт-центр для проверки наличия акции, розыгрыша или опроса.

Как не попасться на уловки мошенников

Все чаще мошенники для получения доступа к персональным данным, реквизитам банковских платежных карточек, паролям и другой конфиденциальной информации используют методы «социальной инженерии»: не взламывают устройства, а выманивают нужную информацию, используя ваши эмоции.

С клиентом банка посредством телефонного звонка или в социальных сетях связывается мошенник под видом представителя банка или с аккаунта друга, родственника. В ходе звонка или переписки собеседник описывает свою сложную жизненную ситуацию и просит ему материально помочь или «запугивает» ложной информацией о сомнительных операциях с банковской карточкой (наличии заявки на кредит, блокировке счета, мошеннических атаках и др.), представляясь работником банка, и предлагает для сохранения оставшихся денежных средств перевести их на новый счет. Собеседник говорит очень убедительно и, как правило, торопит развивающиеся события.

Сценарии могут быть разными, а итог один: клиент самостоятельно предоставляет все секретные данные, коды из смс-сообщений банка, логин и пароли. Поэтому такие случаи не относятся к принципу «нулевой ответственности» банка, так как конфиденциальные данные злоумышленнику сообщили вы сами.

Обезопасить себя от данного типа мошенничества можно, соблюдая простые меры безопасности и проявляя разумную бдительность. Если ваш собеседник представился сотрудником банка и пытается получить персональные данные, рекомендуем незамедлительно завершить диалог и самостоятельно обратиться в банк по номеру, указанному на Вашей банковской карте, официальном сайте либо прийти в офис лично.

Не будьте излишне доверчивыми, не совершайте действий, которые способствуют передаче конфиденциальных данных третьим лицам!

Вот несколько простых советов, соблюдение которых, позволит не стать жертвой злоумышленников:

1. Перед тем, как откликнуться на просьбу друга в социальной сети, созвонитесь с ним или найдите способ убедиться в том, что его аккаунт не взломан (задайте другу вопрос, ответ на который знаете только вы оба);
2. У банков нет совместных контактных центров и служб безопасности, следовательно, переключение между ними невозможно. Если звонящий говорит о таком «переключении», прервите разговор и перезвоните в Банк по номерам, указанным на вашей банковской карте либо официальном сайте финансового учреждения;
3. Если смс-сообщение о подозрительной операции по карточке приходит в новую ветку переписки, в которой ранее не было сообщений от Банка – это повод уточнить ее достоверность и перезвонить в Банк по официальным номерам;
4. Работники банка никогда не просят озвучить смс-код, который необходим для подтверждения совершения банковской операции, а также никогда не спрашивают логин или пароль для входа в систему Интернет-банкинга. В такой ситуации немедленно прервите разговор и свяжитесь с Банком по официальным номерам.
5. Никому не сообщайте данные своей карточки и всегда держите её в поле зрения при совершении платежей;
6. Обязательно подключите 3D-secure и смс-оповещение;
7. Используйте только официальный сайт для входа в систему Интернет-банкинга или официальное мобильное приложение соответствующего банковского учреждения;
8. Регулярно обновляйте пароли, используемые для входа в систему Интернет-банкинга, а также для подтверждения платежей;
9. В случае выявления действий по карточке, которые не совершались ее держателем, необходимо оперативно обратится в Банк по официальным номерам или заблокировать карточку самостоятельно в Интернет/М-банкинге (при наличии такой возможности).

Что бы обезопасить себя и повысить уровень цифровой грамотности, рассмотрим самые распространенные на текущий момент схемы мошенничества:

1. **«Звонок из Банка»**

Вам звонит незнакомец. Номер входящего звонка очень похож на номер банка, а звонящий представляется работником контакт-центра или службы безопасности банка.

Для реализации мошеннической схемы также используются мессенджеры, прежде всего Viber, WhatsApp и Telegram. Входящий звонок максимально закамуфлирован под звонок сотрудника банка: на аватарке может использоваться логотип банка (полностью или частично), а отображаемый телефонный номер звонящего может быть очень похож на телефон службы поддержки банка. У мошенников есть возможность звонить с номеров, похожих (реже – полностью совпадающих) на официальные номера банка. Злоумышленники меняют цифры в номере, которые вы можете не заметить.

Мошенник сообщает, что «банк выявил подозрительную операцию по Вашей карте» или «поступил запрос на онлайн-оформление кредита на Ваше имя».

Он просит у вас логин и пароль от Интернет-банкинга, код из SMS от Банка (зачастую сопровождаемый фразой «Никому не сообщайте!»), реквизиты карты (полный номер карты и срок ее действия, CVV- или CVC-код). Это нужно якобы «для сохранности ваших денег».

Как мошенник пытается вас убедить:

- «*Мы звоним с официального номера, проверьте на сайте».*
- *«В целях конфиденциальности я включаю робота, который защитит ваши данные»*.
- Для убедительности он называет ваши персональные данные (имя, отчество, последние 4 цифры карты и др.) и просит перевести деньги *«на защищённый счет, который закреплён за персональным менеджером: это нужно для безопасности, а потом вы сможете вернуть деньги».*
- Или просит назвать ваши персональные данные или секретные коды из SMS роботу, при этом в трубке вы слышите музыку.
- Вам предлагают услуги страховки от мошеннических действий. Для ее оформления необходимо предоставить данные о карте, на которой находятся значительные денежные средства и SMS-код для подтверждения операции.

Важно! Никому не сообщайте свои личные данные, данные карт, защитные коды, коды из SMS! Если с картой, действительно, происходят мошеннические операции, Банк сам может ее заблокировать!

Еще один из способов получить доступ к Вашим денежным средствам, используя методы социальной инженерии, побудить клиентов банковских учреждений установить сторонние мобильные приложения для удаленного доступа в мобильное устройство потенциальной жертвы. Для примера, одним из таких приложений является “AnyDesk - удаленное управление” из сервисов Google Play/App Store.

Звонки осуществляются, как правило, на мобильные телефоны из указанных выше мессенджеров. При этом мошенники представляются сотрудниками банка, сообщают о якобы зафиксированных попытках совершения подозрительных операций на внушительные суммы, предлагают подтвердить их легитимность. В ходе разговора, с целью скорейшего вхождения в доверие, опрашивают клиента, задавая вопросы общего характера: «Передавалась ли БПК третьим лицам», «Доставляются ли СМС-оповещения» и т.п. Сообщают о блокировке сомнительных операций и счета клиента. Для повышения степени защищенности Интернет-банкинга и восстановления доступа к счету клиенту настоятельно рекомендуют установить приложение «AnyDesk - удаленное управление» из сервисов Google Play/App Store. В случае согласия пострадавшего, конечно же, оказывают помощь и консультацию в установке. Установленное приложение позволяет злоумышленникам получить удалённый доступ к вашему устройству.

2. **«Потенциальный покупатель»**

Мошенник представляется потенциальным покупателем товара, объявление о продаже которого было размещено вами в сети Интернет. По каким-то причинам «покупатель» не может сегодня привезти или перечислить деньги, но хочет прислать вам залог из другого города по системе дистанционного банковского обслуживания.

Для проверки поступления перевода мошенник направляет вам ссылку на фишинговый сайт, который очень близок по дизайну на используемый вами интернет-банк или страницу для ввода реквизитов карточки для получения уже отправленного перевода денежных средств. После введения вами в поля фишингового сайта пароля и логина или реквизитов вашей карточки, данные становятся доступны мошеннику.

Вместо ссылки мошенник может направить вам QR-код, который также хранит в себе ссылку на фишинговый сайт. После введения вами в поля фишингового сайта пароля и логина или реквизитов вашей карточки, данные становятся доступны мошеннику.

Важно! Не переходите по подозрительным ссылкам. Для веб-версии Интернет-банкинга используйте только официальный сайт Банка, а для мобильной версии – только мобильное приложение, загруженное из официальных магазинов. Внимательно изучите сайт, на котором вводите личные данные. Обязательно проверьте наличие такого сайта в Интернете путем обычного поиска.

Запомните! Для получения перевода денежных средств нет необходимости вводить срок действия карты и CVV-код.

3. **«Сообщения в социальных сетях»**

Мошенник незаконным путем получает доступ к страничке в социальной сети и отправляет сообщения с просьбой финансовой помощи от имени ее владельца друзьям.

Просьба может быть самая разная: от «Скинь мне денег на карту, по дружбе» до нехватки денег на большую покупку. В редких случаях мошенник даже просит произвести оплату самостоятельно, обещая возместить затраты при личной встрече.

При получении сомнительного сообщения или малейшей неуверенности в том, что вы действительно общаетесь с владельцем странички, позвоните ему.

4. **«Розыгрыши/раздачи/опросы от Банка или иных организаций»**

Мошенники оставляют выдуманную рекламу в популярных социальных сетях об опросе от имени Банка и «Раздаче призов первой 1000 прошедших опрос!» либо для зачисления денежных средств в честь юбилейной даты со дня образования того или иного финансового учреждения. Цель опроса — изучить мнение клиентов. После прохождения опроса организатор обещает денежное вознаграждение. Однако, по окончанию опроса необходимо заплатить небольшую комиссию, связанную с перечислением вознаграждения или ввести персональные данные Вашей карты для зачисления на нее денежных средств.

Данный кейс очень разнообразен и ограничивается только воображением мошенников. Вместо опроса может предлагаться возмещение налоговых выплат, компенсация за наличие ваших данных в базе «утечки» и иные махинации.

Важно! Посетите официальную страницу организации, а не ресурс, ссылку на который прислал мошенник или позвоните в контакт-центр для проверки наличия акции, розыгрыша или опроса.

5. **«Фишинг и новшества в различных платежах»**

Дополнительно хотим рассказать о новой мошеннической схеме, которая в текущее время широко распространена на территории Российской Федерации и, к сожалению, может быть актуальна для граждан Республики Беларусь.

Злоумышленниками по электронной почте рассылаются фальшивые уведомления об оплате долгов за жилищно-коммунальные услуги, которые возникли за время самоизоляции. В письмах сообщается о задолженности и просьбой оплатить поддельные квитанции онлайн, либо предоставить сведения об уже совершенной оплате. В случае, если клиент начинал производить оплату и вводить реквизиты карточки на сайте, куда его привели ссылки из письма, мошенники получали доступ к его счету. В случае игнорирования клиентом подобных сообщений, ему звонили от лица управляющей компании и убеждали в наличии «долга по квартплате». При этом мошенники пытались выяснить способы оплаты и реквизиты карточки, по которой проводился платёж, и предлагали совершить «тестовую транзакцию для проверки», а также сообщить им код из SMS.

Стоит помнить, что мошенники идут в ногу со временем, а общество постоянно повышает уровень своих цифровых знаний, всё больше узнает о социальной инженерии и иных методах злоумышленников, поэтому используемые сейчас последними способы и средства для хищения денежных средств в скором времени могут стать неактуальными, поэтому в любой ситуации нужно оставаться предельно внимательными и досконально разобраться в случившемся, прежде чем сообщить кому-то свои персональные данные. Ведь Ваша безопасность в первую очередь в Ваших руках!

ОСТОРОЖНО МОШЕННИКИ!

ЗА ЭТИМИ ДАННЫМИ ОХОТЯТСЯ ЗЛОУМЫШЛЕННИКИ

1. **Сеансовые (SMS) одноразовые пароли.** К ним относятся любые секретные коды, которые приходят к Вам в SMS-сообщениях при входе в системы банка. Завладев ими, можно от Вашего имени совершить финансовые операции. ВАЖНО: если Вы передали секретный код, это позволяет изменить данные в Вашем личном кабинете мобильного или интернет-банка.

НИКОМУ НЕ СООБЩАЙТЕ, ДАЖЕ СОТРУДНИКАМ БАНКА,
Ваши сеансовые пароли (код, который банк отправляет в SMS-сообщении)

2. **Реквизиты карты** (имея, например, только номер карты и срок ее действия, можно осуществлять покупки в ряде интернет-магазинов).

3. **Информация**, которую Вы разместили **в сети Интернет** (фотографии (например, фото авиабилетов), номер телефона, адрес, данные паспорта) мошенники могут использовать для формирования доверительного тона и вымогательства у Вас денежных средств.

НИ ПОД КАКИМ ПРЕДЛОГОМ НИКОМУ НЕ СООБЩАЙТЕ

1. **Сеансовые пароли** (секретные коды, которые приходятк Вам в SMS-сообщениях от банка)
2. **ПИН-код** (выданный банком секретный код к карточке)
3. **CVV-код** (3 цифры на обратной стороне Вашей карты)
4. **Логины и пароли, личные паспортные данные**
5. **Номер вашей банковской платежной карточки,** а также срок ее действия

ПРАВИЛА РАБОТЫ В ИНТЕРНЕТЕ

1. Обращайте внимание на корректность написания адреса сайта.
2. Внимательно присматривайтесь к написанию сайта и к существованию специального "Замочка", обозначающего защищенное соединение.
3. Открытый или перечеркнутый замок – безопасность не подтверждена.

Ваша безопасность – в Ваших руках!

Разработано при поддержке Национального банка РБ

7 СХЕМ ОБМАНА

Внимание!
Сосредоточьтесь!

1. Вам может написать/позвонить якобы сотрудник банка и запросить конфиденциальную информацию по вашей карте, логин и пароль от интернет/мобильного банка возможен шантаж и угрозы (ЗАПОМНИТЕ: банк никогда не будет запрашивать Ваши пароли и другие секретные данные).

2. Злоумышленники могут создать точную копию сайта, идентичную оригинальному. Когда Вы введете свои данные, они смогут их получить.

www.21wek.by – w вместо v
www.2lvek.by – l вместо 1
www.21vek.by – оригинальный сайт

3. Переходя по ссылке от незнакомца ("честные" продавцы), Вы подвергаете опасности свои данные и финансы.

4. Установка на Ваше устройство программы-вируса (считывает Ваши данные). Не оставляйте без присмотра Ваши телефоны и другие гаджеты.

5. Сайты-"разводилы" – предлагают сыграть в игру по принципу интернет-казино. Сайты направлены исключительно на то, чтобы завладеть Вашими денежными средствами.

6. Передача телефона третьим лицам.
Под предлогом совершения звонка злоумышленник просит смартфон, устанавливает нанем программное обеспечение, посредством которого осуществляет переводы денежных средств.

7. Кража данных карточек (скимминг — с использованием камер и считывающих устройств на банкоматах).

Разработано при поддержке Национального банка РБ

Как защитить свои сбережения в виртуальном мире

На протяжении текущего года в Республике Беларусь вновь наблюдается рост количества преступлений в сфере информационных технологий. Подавляющее большинство из них составляют хищения денежных средств путем завладения реквизитами банковских платежных карт – ст. 212 (хищение имущества путем модификации компьютерной информации) Уголовного кодекса Республики Беларусь.

Понимание того, что такое киберпреступение, какие типы киберпреступлений существуют и как от них защититься, поможет вам чувствовать себя увереннее.

В этой статье подробно расскажем о том, что такое киберпреступность, от каких угроз и как нужно защищаться, чтобы обеспечить свою безопасности в сети интернет.

Что такое киберпреступление

Киберпреступление - это преступная деятельность, целью которой является неправомерное использование компьютера, компьютерной сети или сетевого устройства.

Большинство киберпреступлений совершаются киберпреступниками или хакерами, которые зарабатывают на этом деньги. Киберпреступная деятельность осуществляется отдельными лицами или организациями.

Некоторые киберпреступники объединяются в организованные группы, используют передовые методы и обладают высокой технической квалификацией. Другие – начинающие хакеры.

Киберпреступники редко взламывают компьютеры по причинам, не имеющим отношения к получению прибыли, например, по политическим или личным.

Типы киберпреступлений

Вот несколько примеров различных типов киберпреступлений:

- Мошенничество с электронной почтой и интернет-мошенничество;
- Мошенничество с использованием личных данных (кража и злонамеренное использование личной информации);
- Кража финансовых данных или данных банковских карт;
- Кража и продажа корпоративных данных;
- Кибершантаж (требование денег для предотвращения кибератаки);
- Атаки программ-вымогателей (тип кибершантажа);
- Криптоджекинг (майнинг криптовалюты с использованием чужих ресурсов без ведома их владельцев);
- Кибершпионаж (несанкционированное получение доступа к данным государственных или коммерческих организаций).

Большинство киберпреступлений относится к одной из двух категорий:

- Криминальная деятельность, целью которой являются сами компьютеры;
- Криминальная деятельность, в которой компьютеры используются для совершения других преступлений.

В первом случае преступники используют вирусы и другие типы вредоносных программ, чтобы заразить компьютеры и таким образом повредить их или остановить их работу. Также с помощью зловредов можно удалять или похищать данные.

Киберпреступления, в результате которых владельцы устройств не могут пользоваться своими компьютерами или сетью, а компании - предоставлять интернет-услуги своим клиентам, называется атакой отказа в обслуживании (DoS).

Киберпреступления второй категории используют компьютеры или сети для распространения вредоносных программ, нелегальной информации или неразрешенных изображений.

Иногда злоумышленники могут совмещать обе категории киберпреступлений. Сначала они заражают компьютеры вирусами, а затем используют их для распространения вредоносного ПО на другие машины или по всей сети.

Киберпреступники могут также выполнять так называемую атаку с распределенным отказом в обслуживании (DDos). Она похожа на DoS-атаку, но для ее проведения преступники используют множество скомпрометированных компьютеров.

Примеры киберпреступлений

Рассмотрим резонансные примеры различных типов кибератак:

1. Атаки с использованием вредоносного ПО

Атака с использованием вредоносного ПО – это заражение компьютерной системы или сети компьютерным вирусом или другим типом вредоносного ПО.

Компьютер, зараженный вредоносной программой, может использоваться злоумышленниками для достижения разных целей.К ним относятся кража конфиденциальных данных, использование компьютера для совершения других преступных действий или нанесение ущерба данным.

Известным мировым примером атаки с использованием вредоносного ПО является атака вымогателя WannaCry, случившаяся в мае 2017 года.Ransomware – это тип вредоносного ПО, который используется для получения денег в обмен на разблокирование устройства/файлов жертвы. WannaCry - это тип программ-вымогателей, которые используют уязвимость компьютеров Windows.Жертвами WannaCry стали 230 000 компьютеров в 150 странах мира. Владельцы заблокированных файлов отправили сообщение с согласием заплатить выкуп в криптовалюте BitCoin за восстановление доступа к своим данным.Финансовые потери в результате деятельности WannaCry оцениваются в 4 миллиарда долларов.

2. Фишинг

Фишинговая кампания – это массовая рассылка спам-сообщений или других форм коммуникации с целью заставить получателей выполнить действия, которые ставят под угрозу их личную безопасность или безопасность организации, в которой они работают.Сообщения в фишинговой рассылке могут содержать зараженные вложения или ссылки на вредоносные сайты. Они также могут просить получателя в ответном письме предоставить конфиденциальную информацию.

Известный пример фишинг-мошенничества произошел на Чемпионате мира по футболу в 2018году. По информации Inc, фишинговые электронные письма рассылались футбольным фанатам.

В этих письмах злоумышленники привлекали болельщиков фальшивыми бесплатными поездками в Москву на Чемпионат мира.У людей, которые проходили по ссылке в сообщениях, были украдены личные данные.

Другой тип фишинговой кампании известен как целевой фишинг. Мошенники пытаются обмануть конкретных людей, ставя под угрозу безопасность организации, в которой они работают.В отличие от массовых неперсонифицированных фишинговых рассылок сообщения для целевого фишинга создаются так, чтобы у получателя не возникло сомнений, что они отправлены из надежного источника, например, от генерального директора или IT-менеджера.

3. Распределённые атаки типа «отказ в обслуживании»

Распределенные атаки типа «отказ в обслуживании» (DDoS) - это тип кибератаки, которую злоумышленники используют для взлома системы или сети. Иногда для запуска DDoS-атак используются подключенные устройства IoT (Internet of Things – Интернет вещей).

DDoS-атака перегружает систему большим количеством запросов на подключение, которые она рассылает через один из стандартных протоколов связи.

Кибершантажисты могут использовать угрозу DDoS-атаки для получения денег. Кроме того, DDoS запускают в качестве отвлекающего маневра в момент совершения другого типа киберпреступления.

Известным примером DDoS-атаки является атака на веб-сайт Национальной лотереи Великобритании в 2017 году. Результатом стало отключение веб-сайта и мобильного приложения лотереи, что не позволило гражданам Великобритании играть.

Как не стать жертвой киберпреступления

Теперь, понимая, какую угрозу представляет киберпреступность, встает вопрос о том, как наилучшим образом защитить ваш компьютер и личные данные?

Следующие советы помогут обезопасить себя и сохранить Ваши деньги:

1. **Регулярно обновляйте ПО и операционную систему**

Постоянное обновление программного обеспечения и операционной системы гарантирует, что для защиты вашего компьютера используются новейшие исправления безопасности.

2. **Установите антивирусное ПО и регулярно его обновляйте**

Использование антивируса или комплексного решения для обеспечения интернет-безопасности,– это правильный способ защитить вашу систему от атак.Антивирусное ПО позволяет проверять, обнаруживать и удалять угрозы до того, как они создадут проблему. Оно помогает защитить ваш компьютер и ваши данные от киберпреступников.Если вы используете антивирусное программное обеспечение, регулярно обновляйте его, чтобы обеспечить наилучший уровень защиты.

3. **Используйте сложные пароли**

Используйте сложные пароли, которые трудно подобрать, и, по возможности, нигде их не записывайте, особенно в цифровом виде. Можно воспользоваться услугой надежного менеджера паролей, который облегчит вам задачу, предложив сгенерированный им сложный пароль.

4. **Не открывайте вложения в электронных спам-сообщениях**

Классический способ заражения компьютеров с помощью вредоносных атак и других типов киберпреступлений - это вложения в электронных спам-сообщениях. Никогда не открывайте вложение от неизвестного вам отправителя.

5. **Не нажимайте на ссылки в электронных спам-сообщениях и на сайтах, которые Вам не знакомы**

Еще один способ, используемый киберпреступниками для заражения компьютеров пользователей, – это вредоносные ссылки в спамовых электронных письмах или других сообщениях, а также на незнакомых веб-сайтах. Не проходите по этим ссылкам, чтобы не стать жертвой интернет-мошенников.

6. **Не предоставляйте личную информацию, не убедившись в безопасности канала передачи**

Никогда не передавайте личные данные по телефону или по электронной почте, если вы не уверены, что телефонное соединение или электронная почта защищены. Убедитесь, что вы действительно говорите именно с тем человеком, который вам нужен.

7. **Свяжитесь напрямую с компанией, если вы получили подозрительный запрос**

Если звонящий просит вас предоставить какие-либо данные, положите трубку. Перезвоните в компанию напрямую по номеру телефона на ее официальном сайте, и убедитесь, что вам звонили не мошенники.Желательно пользоваться, при этом, другим телефоном, потому что злоумышленники могут оставаться на линии: вы будете думать, что набрали номер заново, а они будут отвечать якобы от имени банка или другой организации, с которой, по вашему мнению, вы разговариваете.

8. **Внимательно проверяйте адреса веб-сайтов, которые вы посещаете**

Обращайте внимание на URL-адреса сайтов, на которые вы хотите зайти. Убедитесь, что они выглядят легитимно. Не переходите по ссылкам, содержащим незнакомые или на вид спамовые URL-адреса.Если ваш продукт для обеспечения безопасности в сети интернет включает функцию защиты онлайн-транзакций, убедитесь, что она активирована.

9. **Внимательно просматривайте свои банковские выписки**

Наши советы должны помочь вам не стать жертвой киберпреступников. Но если все же это случилось, важно понять, когда и как это произошло.Просматривайте внимательно свои банковские выписки и запрашивайте в банке информацию по любым незнакомым транзакциям. Банк может проверить, являются ли они мошенническими.

Теперь вы понимаете, какую угрозу представляют киберпреступники, и знаете, как от нее защититься.

Вишинг. Как понять, что вам звонит не банк, а мошенник

Вишинг (англ. *vishing*, от *voice phishing*) — один из методов мошенничества с использованием социальной инженерии, который заключается в том, что злоумышленники, используя телефонную коммуникацию и играя определённую роль (сотрудника банка, покупателя и т. д.), под разными предлогами выманивают у держателя платежной карты конфиденциальную информацию или стимулируют к совершению определённых действий со своим карточным счетом / платежной картой.

Исходя из статистических сведений, с начала 2020 года вишинг набирает все большую популярность и входит в топ самых распространенных способов телефонного мошенничества на территории нашей страны. Результаты многочисленных исследований показывают следующее:

- Во время эпидемии COVID-19 количество звонков от финансовых мошенников выросло более чем на 30%.

- Большинство звонящих в первую очередь пытаются вызвать доверие клиентов. Подавляющая часть мошенников знают, как минимум, имя человека, другие знают также фамилию и отчество,

меньшинство обладают сведениями о персональных данных карты или могут назвать банк, в котором обслуживается клиент. Все эти сведения мошенники используют в беседе, и часто клиенты начинают верить в то, что общаются именно с сотрудником банковской организации.

- Персональную информацию о клиентах мошенники получают благодаря сливам баз данных банков или с помощью агрегаторов данных. Например, ФИО и номера телефонов могут быть у различных магазинов: они собирают информацию о своих покупателях для включения их в бонусные программы. Если мошенник получит доступ к этим данным, он будет знать имя и фамилию клиента, а также номер его телефона.

- Мошенники используют различные техники социальной инженерии, за основу можно выделить несколько сценариев, которыми чаще всего пользуются злоумышленники. Обычно звонящие пытаются сразу вызвать страх у клиентов: сообщают о подозрительном платеже с банковской карты или о том, что карта заблокирована. Реже мошенники звонят с «выгодным» предложением — открыть вклад или получить кредит.

- Целью мошеннических звонков в большинстве случаев являются коды из СМС, приходящие на телефон клиента. Например, если мошенники звонят и говорят, что с карты пользователя был совершен подозрительный перевод без его ведома, то позже они предложат остановить транзакцию. Чтобы ее остановить, злоумышленники попросят клиента назвать код из СМС, которая придет во время разговора. Однако на самом деле клиент не останавливает транзакцию, а подтверждает ее и деньги уходят на счет мошенников. Второй вариант — мошенники попросят клиента самостоятельно перевести деньги с карты на якобы безопасный счет. При этом злоумышленники называют реквизиты собственных карт. Некоторые мошенники заходят еще дальше и уговаривают под различными предлогами клиента установить специальное приложение на телефон, которое, по их словам, защитит деньги пользователей от краж. Но на самом деле с помощью подобных приложений злоумышленники могут узнать пароль от интернет-банкинга клиента и иные персональные данные, а также удаленно управлять мобильным устройством.

Что делать для защиты от мошенников.

В ситуации, когда самый излюбленный способ работы мошенников — звонок от имени якобы сотрудника банка, лучше вообще не вступать в такие разговоры. К сожалению, злоумышленники сейчас активно пользуются IP-телефонией. Это позволяет использовать номера, которые похожи на официальные номера банков. Иногда эти номера и вовсе могут совпадать.

Следующие советы помогут обезопасить себя при встрече с таким методом мошенничества, как вишинг:

- Ни в коем случае не перезванивайте на тот номер, с которого вам поступил звонок. Сами же при звонке в банк набирайте номер, который указан на сайте банка.

- Сотрудник банка и без звонка должен знать:

o вашу фамилию;

o паспортные данные;

o и то, какие карты у вас оформлены;

o сколько денег осталось у вас на карте.

Если кто-то по телефону начинает спрашивать у вас что-то подобное, смело завершайте разговор и сообщайте о подозрительном звонке в банк.

- Есть информация, которую должны знать только вы. Банки никогда не звонят сами и не спрашивают по телефону у клиентов:

- полный номер карточки;

- срок ее действия;

- CVC/CVV;

- логин и пароль к интернет-банкингу;

- кодовое слово, код из СМС-сообщения.

Подобные сведения банк может спросить только в том случае, если клиент позвонил сам и то, это будет только ограниченная информация, а не полные данные, которые у банка и так имеются. Если вам позвонили и просят сказать что-то из вышеперечисленного — перед вами, скорее всего, мошенник.

Если с вашей картой действительно какие-то проблемы, то банк может сам ее заблокировать (такие случаи были, например, когда резко менялась география совершения операций по карте). Но в любом случае все подобные вопросы нужно решать в отделении банка, а не по телефону.

Еще одна уловка мошенников — рассылать СМС или сообщения в соцсетях со ссылками, перейдя по которым, вы сами установите на смартфон или ноутбук вредоносное ПО для воровства персональной информации. Внешне такие лжесообщения очень похожи на реальные сообщения от банков, госорганов, операторов связи или известных магазинов. Сложность еще и в том, что злоумышленники обычно используют сервисы по сокращению интернет-ссылок и выявить подвох гораздо сложнее.

Если вы получили сообщение о выигрыше, прежде чем переходить по ссылке, узнайте, действительно ли был такой розыгрыш и, если ли информация о розыгрыше на официальном сайте. Например, были случаи, когда клиентам обещали подарки к юбилею банка, которое будет только через несколько лет, либо вообще уже давно было.

Подведем итоги и выделим основное.

В любых ситуациях, проводя какие-либо действия с денежными средствами пользователям необходимо соблюдать повышенную осторожность. Банки не запрашивают CVV-коды (с обратной стороны карты) или коды из СМС, а также иную персональную информацию. Кроме того, пользователям нельзя переходить по сомнительным ссылкам из СМС или писем в интернет-ресурсах, социальных сетях и мессенджерах: они могут вести на мошеннические сайты.

По рекомендациям банковских учреждений, клиенты, которым поступает звонок из банка, должны обращать внимание на манеру общения сотрудников. Мошенники постараются всеми способами убедить клиента продолжать разговор. А настоящая служба безопасности банка никогда не будет возражать, если клиент захочет перезвонить позже.

Если мошенники все же украли деньги со счета клиента, нужно в кратчайшие сроки сообщить банку о несанкционированном переводе и заблокировать карту. Если пользователь не нарушил правила безопасности, банки обязаны вернуть клиенту деньги. Однако сложно говорить о возврате, когда

клиент нарушает правила пользования интернет-банком: сообщает свои данные для входа в онлайн-банк и коды подтверждения мошенникам. В таких случаях все зависит от типа транзакции и удалось ли ее остановить антифрод-системам, либо она ушла.

Пользователям, столкнувшимся с неудачной попыткой мошенничества, также рекомендуется обращаться в банк. Таким образом, банк узнает о новых способах мошенничества и их предотвращает. Также имеет смысл сообщать о злоумышленниках операторам связи: у них есть возможность отследить и заблокировать звонки с номеров мошенников.

Успех или неудача вишинговых мошенников практически полностью зависит от просвещённости и грамотности в сфере информационной безопасности граждан. Таком образом, если клиент будет бдителен и осторожен, то вероятность хищения с его карты денежных средств стремиться к нулю.

Вишинг. Как не попасть на уловки кибермошенников

В этой статье мы расскажем более подробно о способе применения наших украденных или случайно утекших данных, который, несмотря на множество предупреждений в СМИ и от банков, по-прежнему приносит легкие деньги мошенникам.

Речь пойдет о **вишинге** (англ. vishing, от Voice phishing) — методе мошенничества с применением социальной инженерии, суть которого заключается в телефонной коммуникации, введении в заблуждение, претворяясь сотрудником банка, покупателем и так далее, и выманивании под разными предлогами у держателя платежной карты конфиденциальной информации или стимулировании к совершению определенных действий со своим банковским счетом и/или платежной картой.

Данный тип мошенничества стал очень активно применяться в отношении граждан Республики Беларусь с 2019 года. Звонят чаще всего со скрытого, похожего на настоящий номер банка либо подмененного с помощью специального программного обеспечения (то есть отображается при звонке настоящий номер банковской службы). Причем стоит отметить очень важный момент, который значительно повышает доверие к мошеннику. Звоня, он уже знает часть или весь номер карточки, услугами какого банка пользуется человек, а также может обратиться по имени и отчеству.

Сразу возникает логичный и резонный вопрос: откуда у мошенника может быть столько информации о человеке? Ответ на него прост, вишинг всегда начинается с получения сведений о будущей жертве. Источники могут быть самые разнообразные:

- **Утечки** клиентских и/или пользовательских баз сайтов, форумов, чатов, сообществ в соцсетях, торговых площадок, онлайн игр, интернет-магазинов, банков и многих других, не обеспечивающих должный уровень защиты для предоставленной информации или торгующие/обменивающиеся ею. Халатное отношение владельцев указанных баз к доверенным данным позволяет злоумышленникам постоянно обновлять и пополнять свои списки жертв, так как сейчас во всем мире, начиная от индивидуального предпринимателя и заканчивая крупными организациями частного и государственного секторов, все собирают и хранят наши персональные данные, в том числе паспортные и банковские, но не все используют их в заявленных целях или защищают как следует.

- Получение сведений из **открытых источников**, например, открытых страниц соцсетей или объявлений торговых площадок. Распространены случаи вишинговых звонков после публикации объявлений якобы по поводу покупки товара.
- **Фишинг.**
- **Облачные хранилища**. Из-за ненастроенных функций приватности, где могут храниться фотографии документов и иные персональные данные.
- **Социальные сети**. На страницах пользователей социальных сетей в открытом доступе находится огромное количество личной информации, данную информацию, пользователи, не задумываясь о последствиях, предоставляют в открытом виде злоумышленникам.
- Различные сомнительные и непроверенные **форумы, площадки, сайты, интернет-магазины, онлайн игры** собирают ваши регистрационные данные о банковских картах и другие, не обеспечивая должный уровень защиты для предоставленной информации либо банально торгуя ею.
- **Кража данных с пользовательских устройств** (телефон, планшет, ПК и т.д.) после заражения вредоносными приложениями, распространяемыми киберпреступниками.

В качестве примера вишинга можно привести случай, когда клиенту одного из банков позвонил неизвестный мужчина и представился сотрудником службы безопасности. Он сообщил о том, что аккаунт интернет-банкинга взломан и сейчас происходит кража денег со счета. Для того, чтобы заблокировать банкинг, необходимо сообщить логин и пароль, а потом для подтверждения того, что именно клиент является владельцем аккаунта, назвать «секретный код», который придет ему на телефон. Испугавшись, клиент сделал все, как просил «сотрудник банка», и после этого ему пришло оповещение о списании со счета крупной суммы денег.

Таким образом, всегда нужно быть начеку и помнить, банкам нет необходимости так поступать, потому что, во-первых, абсолютно вся информация о своих клиентах (счета, номера карт, баланс, коды и т. д.) у них есть, во-вторых, они способны без вашего участия проводить операции по блокировке переводов, счетов, аккаунтов и не только.

В случае возникновения малейшего подозрения, что вы разговариваете не с сотрудником банка, просто завершите разговор и сами перезвоните по номеру телефона с официального сайта для уточнения всех вопросов либо сообщите о попытке украсть у вас данные или деньги. Также, если вам удалось пресечь такую попытку либо преступнику все же удалось получить от вас желаемое, можно обратиться в правоохранительные органы с заявлением о попытке/совершении в отношении вас преступления.

Рекомендации

В современном мире невозможно гарантированно уберечь себя от утечки персональных данных, а, следовательно, и попыток использовать их против нас (обмануть, украсть деньги или подставить), так как в тех или иных ситуациях их предоставление обязательно, а скомпрометирована может быть информационная система любой компании или организации. Но можно значительно снизить вероятность возникновения подобных ситуаций. Достичь этого можно лишь за счет ответственного и внимательного отношения к своим данным:

- Всегда соблюдать меры цифровой гигиены.
- Быть бдительным в отношении передачи и предоставления любых персональных данных.
- Не выкладывать в публичный доступ.
- Не передавать и не отправлять по почте или в мессенджерах сведения из документов, а также их сканы и фотографии сомнительным и непроверенным сервисам, магазинам, организациям, незнакомым людям.
- Постараться исключить случаи пересылки данных даже знакомому и надежному контакту, которому они необходимы, например, для оформления документов, поскольку вы не сможете проследить, будут ли ваши данные переправлены далее посторонним людям. Если альтернативного способа передать данные нет, то после использования отправителю и получателю необходимо удалить их с почтового сервера, а при пересылке сканов и фотографий документа рекомендуется ставить непосредственно на них пометку (например, водяной знак), с какой целью они пересылаются, чтобы сложнее было использовать в преступных целях.

Подведем итоги и выделим основное.

В любых ситуациях, проводя какие-либо действия с денежными средствами пользователям необходимо соблюдать повышенную осторожность. Банки не запрашивают CVV-коды (с обратной стороны карты) или коды из СМС, а также иную персональную информацию. Кроме того, пользователям нельзя переходить по сомнительным ссылкам из СМС или писем в интернет-ресурсах, социальных сетях и мессенджерах: они могут вести на мошеннические сайты.

По рекомендациям банковских учреждений, клиенты, которым поступает звонок из банка, должны обращать внимание на манеру общения сотрудников. Мошенники постараются всеми способами убедить клиента продолжать разговор. А настоящая служба безопасности банка никогда не будет возражать, если клиент захочет перезвонить позже.

Если мошенники все же украли деньги со счета клиента, нужно в кратчайшие сроки сообщить банку о несанкционированном переводе и заблокировать карту. Если пользователь не нарушил правила безопасности, банки обязаны вернуть клиенту деньги. Однако сложно говорить о возврате, когда клиент нарушает правила пользования интернет-банком: сообщает свои данные для входа в онлайн-банк и коды подтверждения мошенникам. В таких случаях все зависит от типа транзакции и удалось ли ее остановить антифрод-системам, либо она ушла.

Пользователям, столкнувшимся с неудачной попыткой мошенничества, также рекомендуется обращаться в банк. Таким образом, банк узнает о новых способах мошенничества и их предотвращает. Также имеет смысл сообщать о злоумышленниках операторам связи: у них есть возможность отследить и заблокировать звонки с номеров мошенников.

Успех или неудача вишинговых мошенников практически полностью зависит от просвещённости и грамотности в сфере информационной безопасности граждан. Таком образом, если клиент будет бдителен и осторожен, то вероятность хищения с его карты денежных средств стремиться к нулю.

Информация по звонкам от имени сотрудников банка, вишинг

В настоящее время на территории Брестской области продолжает наблюдаться активность злоумышленников, которые осуществляют звонки на мобильные телефоны граждан и под видом представителя банковского учреждения Республики Беларусь пытаются завладеть реквизитами их банковских платежных карт, а также иными конфиденциальными данными. Указанные лица сообщают, что необходимо срочно осуществить какие-либо действия с банковской платежной картой, так как кто-то либо пытается похитить с нее денежные средства, либо оформляет кредит или производит подозрительную оплату. Следует отметить, что преступники используют современные возможности сети Интернет (например, возможность «подмены номера»), а также используют для звонков интернет-мессенджеры, в частности «Viber», где в качестве имени пользователя (никнейм) указывают официальный номер банка либо его название, как следствие у потерпевшего на экране

мобильного телефона может отображаться совершенно любой абонентский номер телефона или никнейм, заданный злоумышленником. Это могут быть номера банковских учреждений или иных абонентов, а также наименования реальных финансовых организаций, которые на самом деле никому звонки не осуществляют, а сам звонок по своим внешним признакам ничем не будет подозрительным.

Следует обращать внимание на то, что **сотрудники банковских учреждений в телефонных разговорах никогда не уточняют у своих клиентов конфиденциальную информацию, а номер банковской платежной карты им всегда известен**.

Если Вам поступил такой звонок, то:

- **ни при каких обстоятельствах, никому и никогда не сообщайте информацию о себе или своей банковской платежной карте. Запомните, банк никогда не станет звонить своим клиентам посредством интернет-мессенджеров!** Если Вам будет звонить настоящий сотрудник банка, то он точно будет знать, как минимум номер Вашей банковской платежной карты и никогда не спросит конфиденциальную информацию в телефонном режиме. В случае если с использованием Вашего счета и правда кто-то будет пытаться совершить несанкционированные операции и Банк это заметит, то его сотрудники сперва инициативно заблокируют Вашу банковскую платежную карту, после чего сообщат Вам причину принятого решения (ничего не уточняя) и пригласят в свое учреждения с паспортом для получения наличных денежных средств и написания заявления на перевыпуск карты;

- уточните с кем именно Вы общаетесь, после чего положите трубку и перезвоните на номер телефона, который отображался у Вас на экране (в этом случае Вы свяжитесь именно с тем абонентом, которому принадлежит указанный номер, а не со злоумышленниками, которые его использовали с целью скрыть свой настоящий номер) и уточните суть возникшей проблемы. Скорее всего собеседник сообщит, что Вам вообще не звонил. Современные технологии позволяют подменить номер на экране Вашего телефона на совершенно любой, в том числе заменить его для примера названием учреждения банка;

- если же на Вас оказывается психологическое давление угрозами, что через несколько секунд Вы понесете финансовые потери, кто-то оформит на Вас кредит или что если Вы не сообщите требуемую информацию, то карту вообще заблокируют, не волнуйтесь, это обычная уловка преступников, главная цель которых ввести Вас в состояние неуверенности и страха потерять сбережения. Даже в этом случае не сообщайте никакой информации собеседнику;

- сами перезвоните в свой банк или в круглосуточную службу сервиса, номер которой написан на оборотной стороне Вашей платежной карты и сообщите о случившемся. Скорее всего специалист сообщит Вам, что никаких несанкционированных операций зафиксировано не было, а сотрудник Банка Вам не звонил.

Если же Вы сообщили кому-либо информацию о своей банковской платежной карте, позвоните в свой Банк или примите иные меры к скорейшей ее блокировке. С заблокированного счета Вам без каких-либо затруднений и комиссий выдадут все денежные средства по предъявлению паспорта.

Помните, что если Вы сообщите злоумышленнику реквизиты своей банковской платежной карты, то он сможет распоряжаться всеми средствами на счету, а также оформить на Ваше имя дополнительные кредитные обязательства.

Фишинг. Как выявить мошенника в сети Интернет

В национальном сегменте сети Интернет Республики Беларусь наблюдается значительное повышение мошеннической активности, связанной с использованием фишинговых страниц и даже целых сайтов.

Целью данной разновидности фишинга является получение не только учетных данных от каких-либо сервисов (логин и пароль), но и данных платежной карты (номер, срок действия, имя и фамилия держателя и CVC2/CVV2 код).

Также стоит отметить, что продуманный целевой фишинг не обходится без использования социальной инженерии. Причем если раньше в основном происходила рассылка фишинговых писем на электронную почту, где была возможность блокировать массовые рассылки, то теперь злоумышленники используют еще мессенджеры и социальные сети, что значительно расширяет целевую аудиторию.

В случае успеха злоумышленник может перечислить с карты жертвы некую сумму денег, если на счете будет достаточно средств. А если получит данные для входа в личный кабинет интернет-банкинга, перечислит все деньги со счета, либо, с использованием межбанковской системы идентификации (МСИ), может открыть счета в других банках (о которых жертва длительное время может не знать), для проведения транзитных операций. В худшем случае, оформит онлайн-кредиты, в которых можно снять наличные, перевести или потратить средства онлайн. А через некоторое время жертве придет извещение о задолженности или повестка в суд за неуплату.

Данная мошенническая активность направлена на государственные органы и организации, юридических и физических лиц.

Подделываются различные ресурсы:

- интернет-банкинги банков;
- торговые площадки;
- различные платформы и сервисы, на которых доступна оплата онлайн каких-либо товаров или оказания услуг.

Новые появляются практически сразу после блокировки старых, а схожесть с реальными сайтами порой достигает очень высокого уровня.

В настоящее время наблюдается две **основные фишинговые схемы мошенничества:**

- Злоумышленник выступает в роли продавца (исполнителя услуги).
- Мошенник притворяется покупателем (заказчиком услуги).

У каждой схемы существуют свои модификации, которые позволяют мошенникам, в том числе повторно, обманывать пользователей.

Пример маскировки под площадку Kufar.by

Существуют различные методы и способы, которыми злоумышленники сегодня пытаются обманывать белорусов.

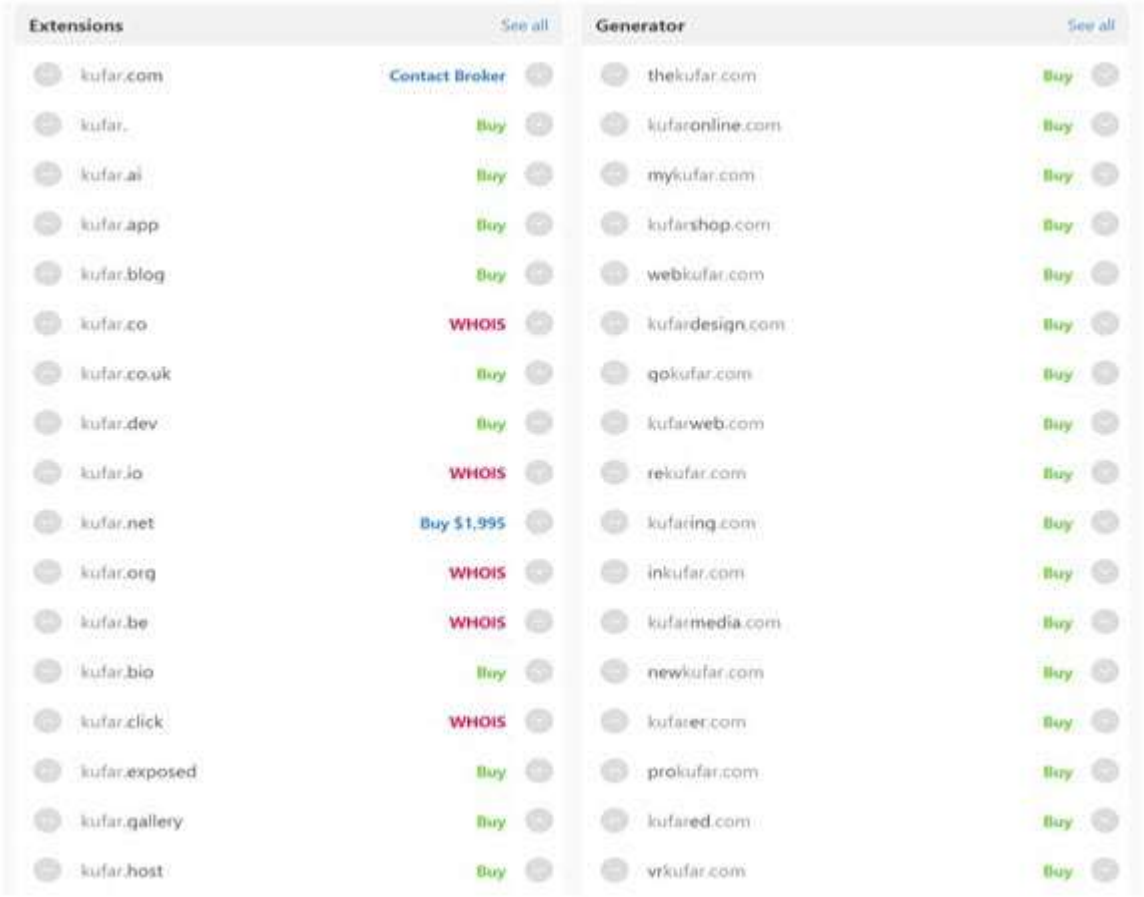
Каждая из схем обмана подразумевает 2 этапа: подготовку и реализацию. Подготовка практически не меняется, в то время как реализация может быть разыграна по-разному.

Все зависит от обстоятельств и того, кто в данный момент выступает в роли жертвы. Мошенники хорошо чувствуют эмоции собеседников, играют на доверчивости и открытости граждан. Могут рассказывать, что попали в сложную жизненную ситуацию и продают вещь за бесценок потому, что нужно оплатить лечение родственнику, учебу ребенку или спасти бизнес, пострадавший от кризиса.

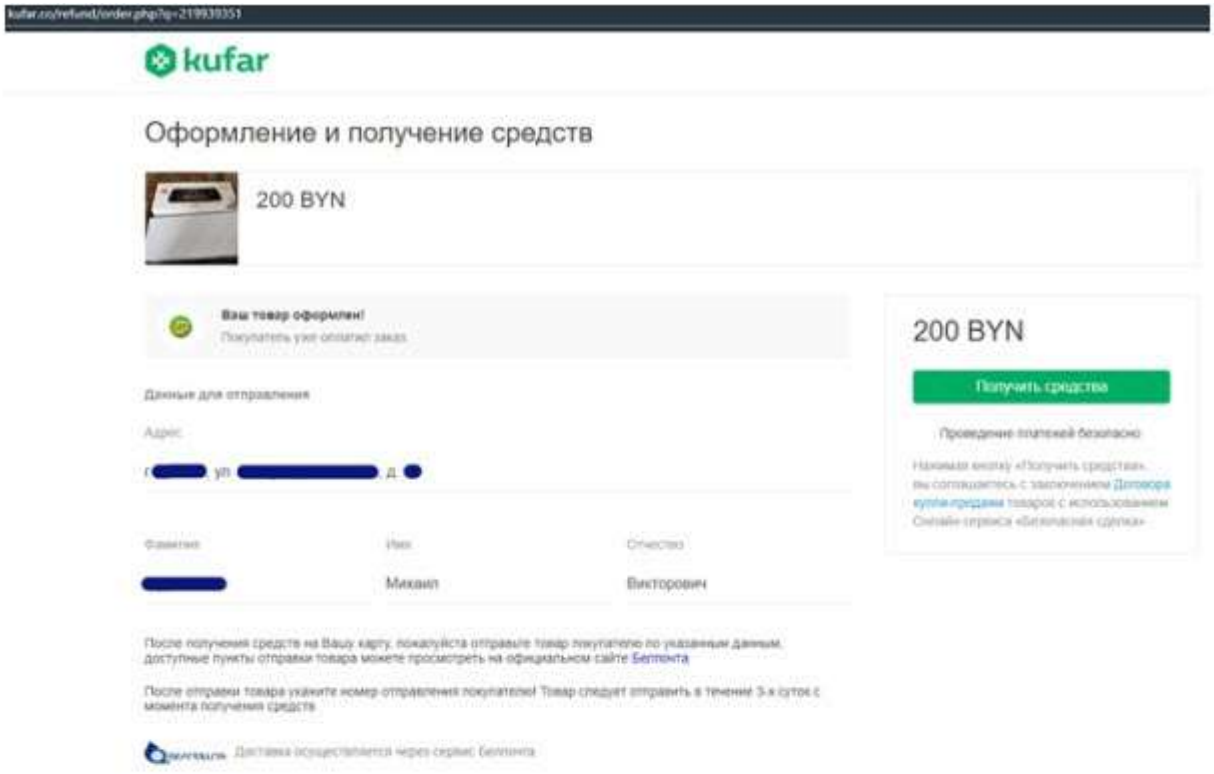
Подготовка:

1. Злоумышленник создает одну страницу, внешне похожую на страницу авторизации официального сервиса, накладную, бланк отправки курьерской службы (платежное обязательство) или же полностью копирует весь сайт.

2. Производит регистрацию домена, визуально схожего с оригинальным. Название может отличаться буквально одним символом либо национальной доменной зоной. Например, пытаясь замаскировать фишинговую страницу под сервис площадки объявлений Kufar.by, злоумышленник может выбрать следующие домены (в списке для сравнения указан и оригинальный домен):

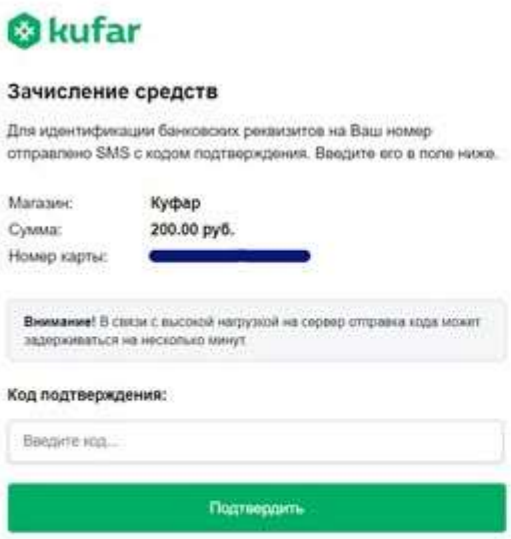


После того, как поддельный сайт создан и размещен на похожем на официальный сайт домене, преступник начинает поиск жертвы.



ПОДДЕЛКА

ПОДДЕЛКА



ПОДДЕЛКА

На данный момент широко используются несколько типичных схем мошенничества. Они направлены как на продавцов, так и на покупателей товаров.

Схема обмана продавцов №1 (Предоплата)

1. Преступник находит продавца на официальной площадке объявлений, копирует его контактные данные, но на площадке не пишет, поскольку пересылка фишинговых ссылок там невозможна. Ищет номер продавца в мессенджерах или пишет в соцсетях, представляясь якобы покупателем с Куфара.

2. Говорит, что уже совершил предоплату. Высылает продавцу ссылку на поддельную страницу, где продавцу нужно ввести номер своей карты для того, чтобы получить деньги. Среди данных, которые просит злоумышленник: номер карты, имя держателя, срок действия, CVV-код на оборотной стороне карты.

3. Иногда мошенник также просит продавца предоставить СМС-код подтверждения платежа, ссылаясь на то, что перевел предоплату и хочет убедиться, что она поступила на счет продавца.

4. С помощью собранных данных мошенник может попытаться перевести с карты жертвы некую сумму денег, и, если на счете будет достаточно средств, ему это удастся.

Схема обмана продавцов №2 (Предоплата)

1. Если предыдущая схема успешно сработала, мошенник может повторно сам связаться с покупателем или представиться службой поддержки и сказать, что произошла ошибка.

2. Чтобы вернуть ошибочно переведенные средства, он предложит перейти на фишинговый сайт и снова ввести данные своей карты.

3. Если продавец это сделает, мошенник может повторно списать деньги.

Схема обмана покупателей №1 (Доставка базовая)

1. Преступник выставляет товар на официальной площадке объявлений по крайне выгодной цене.

2. Когда потенциальный покупатель пишет ему, преступник убеждает перейти в мессенджер или социальную сеть под предлогом того, что там удобнее общаться.

3. Во время общения мошенник уговаривает покупателя на предоплату или доставку под любым предлогом: уехал из города, нет времени.

4. Чтобы развеять сомнения покупателя, говорит о новой услуге холдирования средств, которая появилась на Куфаре: если доставки не будет, Куфар автоматически вернет средства на карту.

5. Высылает покупателю ссылку на поддельную страницу, которая имитирует страницу сервиса «Куфар Доставка» или интернет-банкинга, где нужно ввести данные карты, чтобы совершить предоплату. В качестве данных карты покупателя просят заполнить номер карты, имя держателя, срок ее действия, CVV-код (3 цифры на оборотной стороне карты). В некоторых случаях злоумышленник может попросить назвать проверочный код из СМС-уведомления банка.

6. Как только пользователь вводит данные своей карты, с нее списываются деньги, посылка, естественно, не приходит и средства не возвращаются.

Схема обмана покупателей №2 (Доставка повторная)

1. После того, как предыдущая схема полностью реализована, и покупатель начинает подозревать, что его обманули, мошенник повторно связывается с покупателем.

2. Говорит, что произошла ошибка, товар уже забрали (или передумал подавать), готов вернуть деньги.

3. Высылает ссылку на поддельную страницу возврата средств, где покупателю нужно ввести все те же данные своей карты и точную сумму, которую ему должны вернуть.

4. После того, как покупатель повторно вводит данные своей карты, с его счета повторно списываются деньги.

Схема обмана покупателей №3 (Возврат средств)

1. После того, как мошенник реализовал схему «Доставка», он пишет пострадавшему покупателю, представляется службой поддержки Куфара.

2. Говорит, что посылка была не доставлена, извиняется и рассказывает про возможность возврата средств за посылку.

3. Присылает ссылку на фишинговую страницу, где покупателю снова нужно ввести данные своей карты и сумму, которая соответствовала сумме предыдущего списания.

4. После того, как покупатель повторно вводит данные, мошенник снова крадет деньги с банковского счета.

Схема обмана покупателей №4 (Мошенничество с накладными)

1. Преступник выставляет товар по очень выгодной цене на официальном сайте.

2. Когда потенциальный покупатель пишет ему на Куфаре, под любым предлогом предлагает перейти в мессенджер.

3. Уговаривает отправить товар по почте. При этом мошенник специально создает ажиотаж вокруг объявления. Он может говорить, что буквально на днях уезжает из города, или что товар готовы купить другие покупатели.

4. Продавец говорит, что можно оплатить товар уже после того, как он его отправит, при этом готов предоставить доказательства.

5. Если покупатель соглашается, в качестве доказательства отправки мошенник высылает ссылку на поддельную страницу трекинга посылки или скан поддельного документа об оплате. Минимальное знание фотошопа позволяет преступнику сымитировать квиток любой службы доставки, будь то СДЭК, Белпочта или любая другая компания.

6. После того, как покупатель поверил, что посылка отправлена, мошенник присылает ссылку на фишинговую страницу, где нужно оформить перевод суммы за товар.

7. Как только пользователь вводит данные своей карты, с его счета списываются деньги, а посылка, естественно, не приходит.

Рекомендации:

1. К любым операциям, производимым с использованием Вашей банковской карты, относится максимально внимательно и осторожно. Терять бдительность никогда нельзя.

2. Для оплаты покупок в Интернете завести отдельную карту и не хранить на ней много денег.

3. Если Вам прислали ссылку на почтовый ящик, в мессенджер или SMS-сообщением, то, независимо от того, кто прислал, даже если это Ваш друг, знакомый, государственный орган или организация, с которой Вы постоянно ведете переписку, или абсолютно незнакомый человек, прежде чем ее открывать, следует особенно внимательно проверить доменное имя. При возникновении малейшего сомнения, что ссылка ведет не на официальный ресурс, ее необходимо проверить. Сделать это можно, отыскав в интернете официальный сайт и сверив домен, а также дополнительно проверив информацию о дате регистрации домена (у фишинговых обычно от нескольких дней до нескольких месяцев) на специализированных интернет-ресурсах, например: whois.domaintools.com, centralops.net, xseo.in, cctld.by и других.

4. **Если ресурс оказался поддельным** либо самому не удается определить, то необходимо сделать скриншот фишинговой страницы (чтобы в адресной строке был виден адрес), и отправить в службу поддержки оригинального ресурса, с описанием подробностей ситуации (администрация настоящего ресурса сама заинтересована к недопущению использования своего имени либо логотипов мошенниками), после чего отказаться от проведения каких-либо операций.

5. **Если стали жертвой мошенников:**

- Если ввели данные банковской карты, то необходимо в срочном порядке произвести ее блокировку, позвонив в банк либо, в интернет-банкинге либо три раза введя неверный пароль, с последующей ее заменой.
- Если ввели авторизационные данные от интернет-банкинга, то необходимо немедленно звонить в банк и сообщить о компрометации учетных данных от интернет-банкинга.
- В случае необходимости обратиться в правоохранительные органы с заявлением о мошенничестве.

6. Владельцам **ресурсов** при выявлении случаев мошенничества с использованием фишинговых страниц, мимикрирующих под оригинальный ресурс, или возникновении подозрений о таком использовании:

- Сразу делать скриншоты фишинговых страниц (обязательно чтобы в адресной строке был виден адрес) и переписок с мошенниками.

При необходимости обращаться в соответствующие органы.

Мобильные устройства и безопасность

Мобильные устройства стали неотъемлемой частью нашей повседневной жизни и сопровождают нас во всех делах. В смартфоне мы храним контакты и сообщения, всю переписку во всех социальных сетях. Здесь содержится информация о наших действиях и перемещениях. С помощью смартфона мы пересылаем важные документы и файлы, а также вводим данные банковских приложений и карт. Несмотря на то, что в мобильных устройствах сосредоточена вся наша жизнь, мы не всегда осознаем, сколько ценной личной информации они содержат.

Смартфон — фактически второй компьютер, поэтому прежде всего стоит озаботиться установкой достаточно сложного пароля и автоматической блокировки экрана для предотвращения случайного или намеренного несанкционированного использования данных и приложений на планшете или смартфоне третьими лицами. Используя сложный пароль, вы с меньшей вероятностью станете жертвой мошенников, которые могут воспользоваться тем, что вы оставили телефон без присмотра.

Мобильные устройства подвержены атакам злоумышленников так же, как и персональные компьютеры, а важной информации о вас часто содержат даже больше. Здесь установлены банковские приложения, хранится вся переписка, большая часть ваших фотографий, а иногда — рабочие файлы и данные.

В каждой операционной системе постоянно находят все новые и новые уязвимости — ошибки в ПО, которые создают угрозы для безопасности устройства. Одна из ключевых задач обновлений — решать эти проблемы и повышать уровень безопасности. Злоумышленники ориентируются в первую очередь на тех пользователей, которые пренебрегают простыми правилами безопасности, так как чем современнее версия программы, тем выше уровень защиты. В этой связи стоит регулярно проверять наличие обновлений для приложений, которым пользуетесь, в официальных магазинах приложений и применяйте данные обновления всякий раз, когда они доступны. Используйте функцию автоматического обновления, если не хотите помнить об обновлении приложений или каждый раз делать это вручную.

Точно также, как и на персональном компьютере, при работе с мобильными устройствами стоит опасаться вредоносного программного обеспечения. Существует два основных класса вредоносного ПО, опасного для обычных пользователей:

- программы для перехвата информации (они никак не будут проявлять себя на смартфоне и могут бездействовать довольно долго. Их задача — перехват паролей, данных для онлайн-банкинга, банковских SMS. Иногда эти программы получают сохраненные данные, а иногда перехватывают их в процессе ввода. Если вы не храните в телефоне информацию, которую ПО определяет как интересную, ваше устройство будет использовано как плацдарм для дальнейшего распространения по списку контактов);

- программы-блокировщики экрана (такая программа, оказавшись в смартфоне, выводит на экран свое сообщение, не позволяя пользоваться телефоном. Обычно вредоносное ПО этого типа требует немедленной отправки денег на какой-либо счет, а также SMS на какой-нибудь номер. Часто после этого вас подписывают на мошеннические услуги, или таким образом вы подтверждаете вывод денег со счета).

Кроме этого достаточно широко распространены программы, заставляющие телефон «подслушивать», что говорится рядом, и отсылать аудиозаписи на нужные адреса. Существуют программы, незаметно делающие фото, и программы, отслеживающие местонахождение телефона и отсылающие эти данные мошенникам.

Вредоносная программа может попасть на устройство разными способами:

- Вы получили SMS с подозрительной ссылкой, нажали на нее и перешли на сайт;

- Вы нажали на подозрительную ссылку в браузере — нечаянно или думая, что переходите в какое-то интересное вам место;

- Вы самостоятельно запустили установочный файл .apk на своем Android-устройстве, загрузив его на телефон с компьютера;

- Вы загрузили файл неизвестного производителя, полагая, что устанавливаете нужное приложение;

- Вы активировали анонимный QR-код.

Вас должны настораживать любые неожиданные предложения перейти по ссылке, если вы не полностью уверены в том, что увидите после перехода на сайт. Это может быть:

- ссылка на MMS в SMS;

- непрошеная реклама нового приложения;

- QR-код, кнопка загрузки, замаскированная под интересный текст или красивую картинку, или призыв посмотреть веселый видеоролик.

Принцип действия антивируса на мобильных устройствах совершенно такой же, как и на компьютерах: фильтрация входящих файлов. В этой связи важно обращать внимание на то, что загружается на устройство и всегда помнить, что программы, загруженные с любых сторонних сайтов, проверенных или нет, могут быть заражены вредоносным ПО.

С целью обеспечения личной информационной безопасности и повышения уровня защищенности своих данных помните, что:

- установка «пиратских» приложений может повлечь за собой самые неприятные последствия;

- следует устанавливать только приложения, приобретенные или бесплатно загруженные в официальных магазинах;

- если вы не хотите платить за приложение, воздержитесь от загрузки пиратской версии и найдите бесплатный аналог;

- даже при загрузке приложений из официальных магазинов предварительно их следует проверять антивирусом.

Официальные магазины приложений — вполне безопасное место для поиска и установки необходимого ПО. В официальных магазинах всегда можно посмотреть рейтинг приложения, количество загрузок, а также почитать отзывы, чтобы получить представление о том, что вы собираетесь загрузить и не мошенническое ли это приложение. Кроме этого официальные магазины предоставляют возможность связаться с разработчиком приложения.

Устанавливая любое приложение очень важно обращать внимание на разрешения — действия, которые приложение сможет выполнять после установки. Разрешения у фальшивой программы могут сильно отличаться от разрешений оригинала. Всегда стоит задуматься об установке приложения если Вы даете ему разрешение на отправку смс-сообщений или осуществление звонков, а также на доступ к персональной и финансовой информации, а права администратора обычным приложениям вообще не нужны. Если вы загружаете приложение из официального магазина, про все разрешения можно прочитать подробнее, нажав на галочку около каждого пункта.

Покупки в сети Интернет

Что сегодня может быть проще, чем купить в интернете понравившийся товар? Совершить такую покупку может даже ребенок или пользователь, не вполне уверенно владеющий навыками работы с персональным компьютером. Этот процесс обусловлен тем, что большинство людей сегодня все чаще испытывает дефицит свободного времени и тратить его на походы по магазинам, особенно в поисках обычных товаров, стало для многих недоступной роскошью. Кроме этого, купить или продать товар в сети Интернет стало очень просто благодаря огромному числу торговых площадок, которые делают этот процесс максимально быстрым и удобным, предоставляя возможность оплаты с использованием банковских платежных карт и доставки товара в любой уголок мира.

Согласно исследованиям, рынок электронной коммерции в Республике Беларусь ежегодно растёт и вовлекает все новых пользователей. По статистике, только РУП «Белпочта» обрабатывает около 30 тысяч почтовых отправлений в день, при этом подавляющее большинство наших граждан совершают онлайн-покупки именно на белорусских интернет-площадках.

Такое резкое развитие электронной торговли и большое число людей, вовлеченных в данный процесс, не остались незамеченными злоумышленниками.

В настоящее время наиболее распространены следующие способы совершения противоправных действий с использованием торговых интернет-площадок:

1. **«Предоплата» (обман продавца)**

Суть данного способа заключается в том, что злоумышленник выступает в роли потенциального покупателя товара. На одной из интернет-площадок с объявлениями он находит продавца и копирует его контактные данные. В дальнейшем ищет данного продавца в мессенджерах или пишет в социальных сетях, представляясь якобы покупателем с указанной торговой площадки. В ходе переписки, злоумышленник сообщает, что товар ему понравился и он хочет его приобрести в связи с чем уже якобы совершил предоплату (зачастую высылается скриншот электронного карт-чека о перечислении средств). Для того, чтобы якобы получить данные средства злоумышленник высылает продавцу ссылку на поддельную страницу (зачастую она может выглядеть как один из разделов официального сайта интернет-площадки или банковского учреждения), где продавцу нужно ввести номер своей карты, имя держателя, срок действия, CVV-код указанный на оборотной стороне карты. Кроме этого преступники порой дополнительно просят продавца предоставить информацию, содержащуюся в СМС-сообщении, поступившем из банка, якобы для подтверждения получения предоплаты. После получения конфиденциальных сведений, злоумышленник совершает хищение средств.

Примеры поддельных ресурсов, названия, которых схожи с названием одной из популярных торговых площадок:

2. **«Доставка» (обман покупателя)**

Злоумышленник намеренно размещает объявление на интернет-площадке о продаже товара по крайне выгодной цене. После того, как потенциальный покупатель начинает вести переписку во внутреннем чате площадки, злоумышленник под различными предлогами убеждает его продолжить общение в мессенджере или социальной сети. Во время общения мошенник уговаривает покупателя внести предоплату или оформить доставку, и чтобы развеять сомнения покупателя, злоумышленник сообщает о якобы новой услуге удержания (холдирования) средств, которая появилась на торговой площадке (якобы если доставка не произойдет, то торговая площадка автоматически вернет средства на карту). При этом покупателю высылается ссылку на поддельную страницу, которая имитирует официальную страницу торговой площадки или интернет-банкинга, где нужно ввести данные карты, чтобы совершить предоплату. В качестве данных карты покупателя просят заполнить номер карты, имя держателя, срок ее действия, CVV-код (3 цифры на оборотной стороне карты). В некоторых случаях злоумышленник может попросить назвать проверочный код из СМС-уведомления банка. Как только пользователь вводит данные своей карты, с нее списываются деньги, посылка не приходит и средства не возвращаются.

3. **«Возврат средств» (обман покупателя или продавца)**

После того как злоумышленник использовал одну из описанных выше схем для хищения денежных средств, спустя некоторое время он вновь связывается с потерпевшим (в мессенджерах или социальный сетях), но в этот раз представляется сотрудником торговой площадки или транспортной компании и сообщает, что произошла ошибка и деньги списаны случайно. После этого злоумышленник высылает потерпевшему ссылку на поддельную страницу возврата средств, где нужно вновь ввести данные своей карты и сумму, которую ему якобы должны вернуть. После того, как указанная информация вводится потерпевшим, с его счета повторно списываются деньги.

Для того, чтобы не стать жертвой киберпреступников, совершая сделки в сети Интернет следует:

- вести общение с потенциальными покупателями или продавцами только во внутреннем чате торговой площадки (зачастую торговые площадки блокируют возможность перехода на поддельные ресурсы);

- ведя общение с пользователем стоит перейти к его профилю и обратить внимание на дату создания (если он создан несколько дней назад, то это должно вызвать дополнительную настороженность);

- очень внимательно относится к любому случаю, когда необходимо ввести данные карты или информацию, предоставленную банком (смс-код, логин или пароль от интернет-банкинга). Самый надежный способ уберечь свои средства – это никому не сообщать реквизиты своей карты;

- уточнить у собеседника номер телефона если он не указан в объявлении, а потом позвоните на этот номер, чтобы убедиться, что он реален и принадлежит именно пользователю, с которым вы совершаете сделку (очень часто злоумышленники используют номера телефонов, взятые в аренду на непродолжительное время и физического доступа к нему, не имеют);

- использовать отдельную банковскую карту для осуществления покупок в сети Интернет, на которой не хранятся денежные средства и на которую не поступает регулярный доход в виде заработной платы, стипендии или пенсии;

- избегать перехода по неизвестным интернет-ссылкам, которые предоставляются в ходе переписки якобы для получения предоплаты или оформления доставки. Если Вам прислали такую ссылку, то, независимо от того, кто ее прислал, прежде чем по ней перейти, следует внимательно проверить доменное имя (адрес ресурса). Сделать это можно отыскав в интернете официальный сайт и сверив написание доменного имени. Отличие в одну букву или символ свидетельствует о том, что перед Вами ссылка на поддельный ресурс.

Если Вы все же ввели данные своей банковской карты на поддельном ресурсе или сообщили их постороннему лицу, необходимо в срочном порядке произвести блокировку карты, позвонив в банк либо самостоятельно в интернет-банкинге.

Информация по вредоносному ПО

В настоящее время, на фоне осложнения эпидемиологической обстановки в мире, экспертами в сфере информационной безопасности прогнозируется рост числа рассылок вредоносного программного обеспечения, «фишинговых» писем, а кибератак на компьютеры, оборудование (роутеры, видеокамеры) и незащищенные домашние сети сотрудников организаций, которые перешли на удаленный режим работы. Целью кибератак станет хищение денежных средств или персональных данных пользователей.

С целью получения доступа к безналичным денежным средствам физических и юридических лиц, персональным данным, иной ценной информации, злоумышленники осуществляют фишинговые

рассылки с использованием злободневных тем в том числе о якобы наличии вакцины от актуальных вирусных заболеваний, последних статистических данных или способах борьбы с болезнью. На самом же деле за рассылкой стоят злоумышленники, которые все более изощренными способами используют страхи и сумятицу.

Кроме того, для привлечения внимания потенциальных жертв злоумышленниками могут использоваться реквизиты различных международных благотворительных организаций, а также финансовых учреждений страны. Так, уже зафиксирована вредоносная рассылка с троянской программой внутри, при этом письма отправляются якобы от лица сотрудницы UNICEF — международной организации, действующей под эгидой ООН, а также под видом Всемирной организации здравоохранения. Зачастую к «фейковому» письму прилагался архив, который содержал «троян», совмещающий функционал программы для кражи логинов-паролей и клавиатурного шпиона. Например, он может собирать данные о системе и зараженном компьютере, загружать и запускать файлы, делать скриншоты, управлять клавиатурой и мышью, похищать логины, пароли, а также данные банковских карт.

Для того, чтобы обезопасить свои денежные средства и конфиденциальную информацию, на современном этапе лучше скептически относиться к любым поступающим сообщениям об актуальных вирусных заболеваниях — как об их распространении, так и о средствах защиты, доверяя только крупным надежным источникам, особую внимательность стоит проявлять, получая письмо, содержащее в себе ссылку и текст, призывающий по ней перейти. Чтобы избежать опасности, рекомендуется игнорировать все подобные сообщения и вместо этого заходить на официальный сайт соответствующих организаций или на их страницы в социальных сетях.

Организация безопасной работы в удаленном режиме также имеет свои особенности и требует соблюдения ряда дополнительных требований:

- на персональный компьютер, используемый для работы следует установить лицензионное антивирусное программное обеспечение и произвести его верные настройки, а при работе с электронной почтой следует дополнительно использовать антивирусное программное обеспечение, отвечающее за защиту почтовых сервисов и анализирующие поток данных, проходящий через них;

- при обработке входящей корреспонденции, поступающей по каналам электронной почты следует обращать внимание на прикрепленные к письмам файлы и не допускать их открытия (запуска) непосредственно из почтовой программы. Целесообразно сохранить вложение (не запуская его) и проверить его на наличие вредоносного программного обеспечения. Наличие у поступивших вложений двойного расширения или автоматическое его скрытие может свидетельствовать о прикреплении к файлу вредоносного программного обеспечения;

- USB-ключ с электронной цифровой подписью следует подключать к персональному компьютеру только непосредственно при проведении необходимых финансовых операций;

- заранее позаботьтесь о получении удаленного доступа к необходимым ресурсам и следуйте указаниям специалистов по информационной безопасности своего предприятия для его настройки;

- по возможности работайте на корпоративном компьютере. Постарайтесь не загружать и не открывать корпоративные файлы на личных устройствах;

- домашние сети не защищаются специалистами по информационной безопасности предприятия, поэтому будьте внимательны – атакующие могут воспользоваться ситуацией и направить усилия на менее защищенных пользователей;

- проверьте, настроена ли двухфакторная аутентификация в почте, в мессенджерах и при VPN подключении;

- обязательно смените стандартный пароль домашнего роутера, иначе злоумышленники легко смогут получить доступ к вашим данным;

- объясните близким, что Вашим рабочим компьютером пользоваться нельзя, чтобы избежать случайного заражения устройства или потери данных.

Безопасное использование электронной почты

Сегодня доступ в интернет имеет практически каждый. Кому-то он необходим для выполнения служебных обязанностей, кто-то использует его для учебы, для игр и просмотра фильмов, но практически всех активных пользователей глобальной сети объединяет одно — использование электронной почты.

При быстром ритме современной жизни электронная почта стала важным средством коммуникации. Используя электронную почту, мы можем моментально отправлять и получать письма, документы, программы, фотографии, любые файлы. Кроме того, для регистрации на большинстве ресурсов требуется привязка Вашей электронной почты.

Однако не стоит забывать, что по электронной почте могут приходить не только «полезные» письма. Они могут содержать ссылки на сайты злоумышленников, целью которых является выведать у пользователя важную информацию, или вредоносные файлы, которые, попав на компьютер, могут доставить много неприятностей.

Основной мотив злоумышленника — получение денег. Используя электронную почту в качестве инструмента для совершения злонамеренных действий, он может:

- продавать взломанные аккаунты для рассылки спам-сообщений;

- использовать взломанный аккаунт электронной почты для восстановления паролей других учетных записей, при регистрации которых использовался взломанный адрес (банкинг, соцсети, игровые аккаунты и т.п.)

- использовать информацию из личной или деловой переписки в различных схемах мошенничества;

- вымогать деньги, шантажируя владельца аккаунта;

- рассылать спам-сообщения с адреса взломанной электронной почты.

Использование электронной почты без соблюдения определенных мер безопасности может угрожать безопасности вашего компьютера и тем самым нанести вред вам.

Письма, приходящие по электронной почте, могут содержать вредоносные файлы или ссылки, ведущие на зараженные сайты. При открытии такого файла или переходе по ссылке вирус попадает на компьютер пользователя.

Для защиты компьютера от заражения вирусом необходимо:

- установить на компьютер средство антивирусной защиты и регулярно обновлять антивирусные базы;

- регулярно обновлять операционную систему и программное обеспечение, установленные на компьютере;

- не переходить по ссылкам из подозрительных писем;

- не открывать письма с вложениями, полученные от неизвестных отправителей.

Злоумышленник может попытаться угадать пароль от электронной почты путем перебора наиболее часто встречающихся комбинаций, например 12345, qwerty, p@ssw0rd и т.п., сейчас в открытом доступе можно найти огромное количество собранных баз данных с десятками и сотнями тысяч наиболее часто используемых паролей. Пароли, состоящие из фамилии, даты рождения, номера телефона также могут быть легко угаданы. Подобрав пароль, злоумышленник получает полный доступ к почте жертвы.

Чтобы оградить свою электронную почту от рук злоумышленника, рекомендуется:

- создать сложный пароль;

- менять пароли;

- не хранить пароль на компьютере;

- не использовать основной адрес электронной почты для регистрации на каких-либо ресурсах;

- придумать разные пароли для разных сайтов;

- указать контрольный вопрос и номер телефона для восстановления пароля электронной почты.

Для восстановления пароля электронной почты рекомендуется выбрать контрольный вопрос и задать для него ответ. Однако стоит помнить, что если ответ на контрольный вопрос будет очевидным, то злоумышленник сможет легко его угадать.

Рекомендуется использовать уникальный вопрос и легко запоминающийся ответ, который будете знать только вы и который трудно угадать.

По электронной почте могут приходить письма, якобы от лица администратора соцсети или от сотрудников банка — с просьбой прислать свои логин и пароль, например якобы для восстановления после сбоя базы данных, или с просьбой перейти по ссылке для подтверждения адреса электронной почты. Зачастую, перейдя по ссылке, можно обнаружить запрос на ввод данных (пароля, логина, номера банковской карты и т. п.). При этом страница сайта внешне может быть похожа на ресурс, которым вы привыкли пользоваться (соцсеть, интернет-банкинг). Однако если обратить внимание на адрес такой страницы, то можно заметить, что он незначительно отличается от оригинального, например вместо «o» может стоять «0» или вместо «l» — «I».

Как только запрашиваемые данные будут введены на такой лжестранице, они сразу же попадут в руки злоумышленника, который сможет воспользоваться ими в своих корыстных целях.

Для того чтобы этого избежать, необходимо руководствоваться несколькими простыми правилами:

- не отвечайте на письма от неизвестных отправителей;

- не переходите по ссылкам, содержащимся в письмах;

- не сообщайте приватную информацию, запрашиваемую в письмах, приходящих по электронной почте.

Не рекомендуется сообщать пароль от почты кому бы то ни было. Если в какой-то момент вам пришлось предоставить друзьям или коллегам доступ к своему электронному ящику или если у вас возникло подозрение, что кто-то посторонний узнал ваш пароль, — необходимо как можно скорее его сменить.

При подключении к незащищенным точкам доступа передаваемые данные не шифруются, поэтому злоумышленник может перехватить их при помощи ноутбука с Wi-Fi-адаптером. Используя специальную программу для «перехвата трафика», злоумышленник сможет увидеть все данные, передаваемые по такой сети, в частности пароль от электронной почты.

Для того чтобы обезопасить себя от перехвата паролей рекомендуется:

- не пользоваться открытыми Wi-Fi-сетями для доступа к электронной почте, соцсетям и прочим ресурсам, требующим ввода пароля;

- использовать VPN при подключении к открытым точкам доступа Wi-Fi;

- отключить общий доступ к файлам на устройстве.

Если не соблюдать указанные выше рекомендации, взлом почтового ящика может стать для Вас неприятным сюрпризом.

Скорее всего, ваш почтовый ящик взломали, если:

- не удается войти в электронную почту (пароль не подходит);

- вам сообщили, что с вашего адреса приходят письма, которых вы не отправляли (или в папке «Отправленные» появились такие подозрительные письма);

- исчезли письма, которых вы не удаляли;

- письма, которых вы не читали, помечены как прочитанные;

- установлен пароль на папку «Входящие».

В этом случае необходимо:

- проверить компьютер на вирусы;

- попробовать восстановить пароль по секретному вопросу, с помощью дополнительного адреса или номера мобильного телефона (если это удастся, нужно немедленно сменить пароль и секретный вопрос);

- обратиться в службу поддержки и сообщить о проблеме.

Фишинг и как ему противостоять

Фишинг (англ. *phishing* от *fishing* «*рыбная ловля, выуживание*») — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам, паролям и иной персональной информации. Это достигается путём проведения массовых рассылок электронных писем от имени различных организация, а также личных сообщений внутри сервисов, например, от имени банков или посредством социальных сетей и мессенджеров. В письме зачастую содержится прямая ссылка на сайт, внешне неотличимый от настоящего, либо на сайт с редиректом (перенаправлением). После того как пользователь попадает на поддельную страницу, мошенники пытаются различными психологическими приёмами побудить пользователя ввести на поддельной странице свои логин и пароль, которые он использует для доступа к определённому сайту, реквизиты банковских платежных карт или иные персональные данные, что позволяет мошенникам получить доступ к аккаунтам и банковским счетам.

Таким образом, ***фишинг — одна из разновидностей социальной инженерии, основанная на незнании пользователями основ сетевой безопасности***. В частности, многие не знают простого факта: сервисы не рассылают писем с просьбами сообщить свои учётные данные, пароль и иную информацию, а в мессенджерах нельзя получить денежный перевод путем перехода по ссылке.

Большинство методов фишинга сводится к тому, чтобы замаскировать поддельные ссылки на фишинговые сайты под ссылки настоящих организаций. Адреса с опечатками или субдомены часто используются мошенниками. Например «www.kufar.be», «www.bel-post.by» или «www.belarusbank-erip.cc» визуально похожи на адреса реальных организаций, однако на самом деле они ссылается на

фишинговые составляющие сайтов «www.kufar.by», «www.belpost.by» и «www.belarusbank.by», соответственно.

Другая распространённая уловка заключается в использовании на иных неофициальных ресурсах внешне правильных ссылок, в реальности ведущих на фишинговый сайт из-за измененного атрибута html-ссылки (использование в HTML-теге <a> значения href, отличного от текста ссылки).

Ещё одна проблема была обнаружена при обработке браузерами интернациональных доменных имён (содержащие символы национальных алфавитов, например: «115.бел», «президент.рф» и т.п.): адреса, визуально идентичные официальным, могли вести на сайты мошенников.

Обман не заканчивается на посещении жертвой фишингового сайта. Некоторые фишеры используют JavaScript для изменения адресной строки. Это достигается либо путём размещения картинки с поддельным URL поверх адресной строки либо закрытием настоящей адресной строки и открытием новой с поддельным URL.

Злоумышленник может использовать уязвимости в скриптах подлинного сайта. Этот вид мошенничества (известный как межсайтовый скриптинг) наиболее опасен, так как пользователь авторизуется на настоящей странице официального сайта, где всё (от веб-адреса до сертификатов) выглядит подлинным. Подобный фишинг очень сложно обнаружить без специальных навыков. Данный метод применялся в отношении такой крупной компании, как PayPal еще в 2006 году.

Сегодня фишинг выходит за пределы интернет-мошенничества, а поддельные веб-сайты стали лишь одним из множества его направлений. Письма, которые якобы отправленные из банка, могут сообщать пользователям о необходимости позвонить по определённому номеру для решения проблем с их банковскими счетами. Эта техника называется вишинг (голосовой фишинг). Позвонив на указанный номер, пользователь заслушивает инструкции автоответчика, которые указывают на необходимость ввести или сказать номер своего счёта, банковской карты, PIN-код или иную информацию. К тому же вишеры могут сами звонить жертвам, убеждая их, что они общаются с представителями официальных организаций, используя фальшивые номера. В конечном счёте, человека также попросят сообщить его учётные данные.

Набирает свои обороты и SMS-фишинг, также известный как смишинг (англ. *SMiShing* — от *«SMS»* и *«фишинг»*). Мошенники рассылают сообщения, содержащие ссылку на фишинговый сайт, — входя на него и вводя свои личные данные, жертва аналогичным образом передаёт их злоумышленникам. В сообщении также может говориться о необходимости позвонить мошенникам по определённому номеру для решения «возникших проблем». Иногда смишинг может предшествовать вишингу, например злоумышленники отправляют sms-сообщение на телефон жертвы от имени банка о попытке транзакции с карты, а потом звонят, представляясь уже сотрудником того же банка и предлагают отменить указанный, якобы мошеннический перевод, для чего просят предоставить реквизиты банковской карты или иную персональную информацию клиента, которая настоящему сотруднику банка и так должна быть известна.

Как не попасться на уловки фишеров?

Один из методов борьбы с фишингом заключается в том, чтобы научить людей различать фишинг и бороться с ним. Люди могут снизить угрозу фишинга, немного изменив своё поведение. Так, в ответ на письмо с просьбой «подтверждения» учётной записи (или любой другой обычной просьбой фишеров) необходимо связаться с компанией, от имени которой отправлено сообщение, для проверки его подлинности. Кроме того, рекомендуется самостоятельно вводить веб-адрес организации в адресную строку браузера вместо использования любых гиперссылок в подозрительном сообщении.

Практически все подлинные сообщения организаций содержат в себе упоминание некой информации, недоступной для фишеров. Некоторые, например, всегда обращаются к своим адресатам по именам, а письмо с общим обращением «Уважаемый клиент» может расцениваться как попытка фишинга, однако, даже к электронным письмам, содержащим более подробные данные о себе необходимо относиться с опаской, т.к. эта информация также может стать известна мошенникам иными путями. Письма от банков и кредитных учреждений часто содержат в себе часть номера счёта. Однако, люди не различают появление первых или последних цифр счёта, в то время как первые цифры могут быть одинаковы для всех клиентов финансового учреждения. Людям можно объяснить, что подозрительны любые письма, не содержащие какой-либо конкретной личной информации, но фишинговые атаки могут содержать подробную персональную информацию, следовательно, наличие такого рода сведений не гарантирует безопасность сообщения. Кроме того, статистические показатели гласят, что присутствие личной информации существенно не изменяет процент успеха фишинговых атак, что свидетельствует о том, что большинство людей вообще не обращает внимания на подобные детали.

Стоит помнить, что мошенники идут в ногу со временем, поэтому обычные методы фишинга в скором времени могут стать не актуальными, поскольку люди всё больше узнают о социальной инженерии, используемой фишерами, поэтому в любой ситуации нужно оставаться предельно внимательными и досконально разобраться в случившемся, прежде чем сообщить кому-то свои персональные данные.

Фишинг (англ. *phishing* от *fishing* «*рыбная ловля, выуживание*») — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам, паролям и иной персональной информации. Это достигается путём проведения массовых рассылок электронных писем от имени различных организация, а также личных сообщений внутри сервисов, например, от имени банков или посредством социальных сетей и мессенджеров. В письме зачастую содержится прямая ссылка на сайт, внешне неотличимый от настоящего, либо на сайт с редиректом (перенаправлением). После того как пользователь попадает на поддельную страницу,

мошенники пытаются различными психологическими приёмами побудить пользователя ввести на поддельной странице свои логин и пароль, которые он использует для доступа к определённому сайту, реквизиты банковских платежных карт или иные персональные данные, что позволяет мошенникам получить доступ к аккаунтам и банковским счетам.

Таким образом, ***фишинг — одна из разновидностей социальной инженерии, основанная на незнании пользователями основ сетевой безопасности***. В частности, многие не знают простого факта: сервисы не рассылают писем с просьбами сообщить свои учётные данные, пароль и иную информацию, а в мессенджерах нельзя получить денежный перевод путем перехода по ссылке.

Большинство методов фишинга сводится к тому, чтобы замаскировать поддельные ссылки на фишинговые сайты под ссылки настоящих организаций. Адреса с опечатками или субдомены часто используются мошенниками. Например «www.kufar.be», «www.bel-post.by» или «www.belarusbank-erip.cc» визуально похожи на адреса реальных организаций, однако на самом деле они ссылается на фишинговые составляющие сайтов «www.kufar.by», «www.belpost.by» и «www.belarusbank.by», соответственно.

Другая распространённая уловка заключается в использовании на иных неофициальных ресурсах внешне правильных ссылок, в реальности ведущих на фишинговый сайт из-за измененного атрибута html-ссылки (использование в HTML-теге <a> значения href, отличного от текста ссылки).

Ещё одна проблема была обнаружена при обработке браузерами интернациональных доменных имён (содержащие символы национальных алфавитов, например: «115.бел», «президент.рф» и т.п.): адреса, визуально идентичные официальным, могли вести на сайты мошенников.

Обман не заканчивается на посещении жертвой фишингового сайта. Некоторые фишеры используют JavaScript для изменения адресной строки. Это достигается либо путём размещения картинки с поддельным URL поверх адресной строки либо закрытием настоящей адресной строки и открытием новой с поддельным URL.

Злоумышленник может использовать уязвимости в скриптах подлинного сайта. Этот вид мошенничества (известный как межсайтовый скриптинг) наиболее опасен, так как пользователь авторизуется на настоящей странице официального сайта, где всё (от веб-адреса до сертификатов) выглядит подлинным. Подобный фишинг очень сложно обнаружить без специальных навыков. Данный метод применялся в отношении такой крупной компании, как PayPal еще в 2006 году.

Сегодня фишинг выходит за пределы интернет-мошенничества, а поддельные веб-сайты стали лишь одним из множества его направлений. Письма, которые якобы отправленные из банка, могут сообщать пользователям о необходимости позвонить по определённому номеру для решения проблем с их банковскими счетами. Эта техника называется вишинг (голосовой фишинг). Позвонив на указанный номер, пользователь заслушивает инструкции автоответчика, которые указывают на необходимость ввести или сказать номер своего счёта, банковской карты, PIN-код или иную информацию. К тому же вишеры могут сами звонить жертвам, убеждая их, что они общаются с представителями официальных организаций, используя фальшивые номера. В конечном счёте, человека также попросят сообщить его учётные данные.

Набирает свои обороты и SMS-фишинг, также известный как смишинг (англ. *SMiShing* — от *«SMS»* и *«фишинг»*). Мошенники рассылают сообщения, содержащие ссылку на фишинговый сайт, — входя на него и вводя свои личные данные, жертва аналогичным образом передаёт их злоумышленникам. В сообщении также может говориться о необходимости позвонить мошенникам по определённому номеру для решения «возникших проблем». Иногда смишинг может предшествовать вишингу, например злоумышленники отправляют sms-сообщение на телефон жертвы от имени банка о попытке транзакции с карты, а потом звонят, представляясь уже сотрудником того же банка и предлагают отменить указанный, якобы мошеннический перевод, для чего просят предоставить

реквизиты банковской карты или иную персональную информацию клиента, которая настоящему сотруднику банка и так должна быть известна.

Как не попасться на уловки фишеров?

Один из методов борьбы с фишингом заключается в том, чтобы научить людей различать фишинг и бороться с ним. Люди могут снизить угрозу фишинга, немного изменив своё поведение. Так, в ответ на письмо с просьбой «подтверждения» учётной записи (или любой другой обычной просьбой фишеров) необходимо связаться с компанией, от имени которой отправлено сообщение, для проверки его подлинности. Кроме того, рекомендуется самостоятельно вводить веб-адрес организации в адресную строку браузера вместо использования любых гиперссылок в подозрительном сообщении.

Практически все подлинные сообщения организаций содержат в себе упоминание некой информации, недоступной для фишеров. Некоторые, например, всегда обращаются к своим адресатам по именам, а письмо с общим обращением «Уважаемый клиент» может расцениваться как попытка фишинга, однако, даже к электронным письмам, содержащим более подробные данные о себе необходимо относиться с опаской, т.к. эта информация также может стать известна мошенникам иными путями. Письма от банков и кредитных учреждений часто содержат в себе часть номера счёта. Однако, люди не различают появление первых или последних цифр счёта, в то время как первые цифры могут быть одинаковы для всех клиентов финансового учреждения. Людям можно объяснить, что подозрительны любые письма, не содержащие какой-либо конкретной личной информации, но фишинговые атаки могут содержать подробную персональную информацию, следовательно, наличие такого рода сведений не гарантирует безопасность сообщения. Кроме того, статистические показатели гласят, что присутствие личной информации существенно не изменяет процент успеха фишинговых атак, что свидетельствует о том, что большинство людей вообще не обращает внимания на подобные детали.

Стоит помнить, что мошенники идут в ногу со временем, поэтому обычные методы фишинга в скором времени могут стать не актуальными, поскольку люди всё больше узнают о социальной инженерии, используемой фишерами, поэтому в любой ситуации нужно оставаться предельно внимательными и досконально разобраться в случившемся, прежде чем сообщить кому-то свои персональные данные.

Что делать, если поступило sms о списании средств со счета в адрес интернет-ресурса

На фоне значительного роста мошенничества в сети Интернет, недобросовестные злоумышленники любыми способами пытаются завладеть денежными средствами, хранящимися у Вас на банковских картах. Многие полагают, что преступники переводят похищенные у жертвы средства на находящиеся у них в пользовании платежные карты, счета либо электронные кошельки, однако это не всегда так, в зависимости от случая, обналичить денежные средства можно различными путями, в том числе путем оплаты в сети Интернет товаров и услуг.

В настоящее время в Интернете можно найти практически всё, именно поэтому «глобальная паутина» стала настолько популярной. За развивающейся тенденцией следят крупные компании и предприятия, которые для удобства и более широкого охвата потребителей адаптировались и также перенесли свои услуги в сеть. Теперь, привычные печатные СМИ, телевидение и т.п. постепенно теряют свою популярность, так как все это сейчас можно открыть и просмотреть на соответствующем сайте из любой точки мира. Как в реальном мире, так и в виртуальном пространстве за различные сервисы и услуги тоже приходится платить. Поэтому, сейчас распространены покупки и подписки на различные интернет-сервисы. Так, чтобы просматривать телевидение, пользоваться музыкальными сервисами, приложениями или получать дополнительные бонусы в играх со своего гаджета, будь то это ноутбук, компьютер, телевизор, планшет или телефон, необходимо осуществить платную подписку на указанные услуги.

Мошенники знают все уловки оплаты услуг в сети, поэтому получив данные вашей банковской карты и sms-код подтверждения, могут осуществить платную подписку на какой-либо сервис привязав вашу карту.

Однако, в списаниях денежных средств со счета таким путем в большинстве случаев вина лежит на невнимательности самого пользователя и человеческом факторе. Зачастую люди не читают пользовательское соглашение и ставят галочку о том, что ознакомлены с условиями последнего, где указаны все важные моменты, на которые стоит обратить внимание. Например, некоторые сервисы оказывают не единовременную услугу, а периодично ее предоставляют, за что, соответственно периодично списывается с привязанной карты определенная сумма.

Статистические данные по вышеуказанным фактам говорят о значительном количестве обращений и заявлений граждан в правоохранительные органы, по окончанию рассмотрения которых становится известным, что заявитель сам осуществил подписку на тот или иной сервис и потом попросту забыл об этом, тем временем денежные средства продолжали списываться со счета. Также к не меньшему количеству случаев причастны дети, которые воспользовавшись банковской картой родителя осуществляли подписку на платные сервисы либо совершали внутриигровые покупки.

В последнее время на большую долю мобильных устройств приходится установленная операционная система Android, обеспечение работы которой осуществляет корпорация «GoogleInc.». Поэтому осуществление покупок, в том числе внутриигровых, на указанных устройствах проходит в большинстве случаев посредством сервиса Google Pay.

Рассмотрим подробнее тематику проведения транзакций через Google Pay, их представление в выписке по банковскому счету и вопрос возврата ошибочно списанных средств.

Прежде чем прейти к дальнейшему рассмотрению темы, нужно учитывать, если вы обнаружили в выписке ошибочное списание средств на оплату продуктов (в т.ч. товаров и услуг) Google, которые вы не приобретали, можете оспорить его, заполнив соответствующую форму на сайте: «pay.google.com/payments/unauthorizedtransactions».

В выписке по банковскому счету названия транзакций, проведенных для оплаты товаров и услуг Google, начинаются со слова GOOGLE*, далее указывается продукт или его описание.

Ниже представлены примеры того, как могут называться такие транзакции (обратите внимание, что иногда текст может отображаться с сокращениями):

Название позиции в выписке	**Продукт Google**
GOOGLE *{Компания}	Google Play (приложения)
GOOGLE *CLOUD_{BAID}	Google Cloud
GOOGLE *Commerce Ltd	Google Play Музыка
GOOGLE *{Разработчик}	Google Play (приложения)
GOOGLE *Devices	Google Store
GOOGLE *Domains	Google Domains
GOOGLE *GOOGLE	YouTube Premium
GOOGLE *Google, Inc.	Google Play Музыка
GOOGLE *Google Music	Google Play Музыка
GOOGLE *Google Play	Google Play Фильмы
GOOGLE *Google Storage	Google Диск
GOOGLE *Google Store	Google Store
GOOGLE *Google Surveys	Google Аналитика
GOOGLE *GoogleShopping	Google Покупки.
GOOGLE *Music	Google Play Музыка
GOOGLE *Google Storage	Google One
GOOGLE *Play	Google Play (приложения)
GOOGLE *Play Credit	Подарочные карты Google Play и другие инструменты для зачисления средств на баланс Google Play
GOOGLE *Play Newsstand	Google Play Пресса
GOOGLE *PROJECT FI	Google Project Fi
GOOGLE *SERVICES	Google Fiber YouTube TV
GOOGLE GSUITE {первые 7 букв доменного имени}	G Suite
GOOGLE *Voice	Google Voice
GOOGLE *PAY	Google Pay
GOOGLE *YouTube Videos	Канал "Фильмы и шоу" на YouTube
GOOGLE *TEMPORARY HOLD	Платёж, ожидающий подтверждения. Когда транзакция будет обработана, запись исчезнет. Средства при этом списаны не будут.

В названиях транзакций, проведенных через Google Pay для оплаты сторонних товаров и услуг, приводится имя продавца. Обращаться с вопросами о списании нужно уже к нему.

Таким образом, если вы заметили списание денежных средств с банковской карты, просмотрев как выглядит описание указанной транзакции в выписке по счету, можно определить в адрес какого конкретного ресурса они были перечислены. Если указанную транзакцию вы, ваши дети и близкие

не совершали, можно возвратить денежные средства путем заполнения анкеты на указанном выше сайте.

Стоит помнить, что в любой ситуации нужно оставаться предельно бдительными и внимательными.

Рекомендации безопасных покупок на торговых интернет-площадках:

Обратите внимание на особенности товара

Потертости, небольшие дефекты — уточните эти нюансы у продавца.

Приобретайте вещи при личной встрече

Так вы сможете детально осмотреть и оплатить товар на месте.

Проверьте достоверность номера телефона

Если продавец не предоставляет свои данные, откажитесь от сделки.

Не вносите предоплату

Если продавец вызывает у вас хоть малейшие подозрения.

Сохраняйте важную информацию

Имя продавца, детали переписки, документы, подтверждающие оплату.

Снимите на камеру вскрытие посылки

Снимите видео момента вскрытия посылки и проверки качества содержимого.

Ни при каких обстоятельствах никому не сообщайте ваши паспортные данные, баланс и полные данные карты с CVC/CV2 кодом или кодом из SMS.
Даже если вам обещают перевести деньги.

Рекомендации по безопасности в цифровом пространстве

Рассмотрим основные уловки кибермошенников, а также рекомендации по противодействию последним:

1. Клонирование SIM-карты.

Информация с SIM-карты оператора сотовой подвижной электросвязи, которая попала в руки злоумышленника, может быть скопирована (клонирована) в память компьютера, а потом перенесена на «чистую» SIM-карту. После чего она может быть вывезена за границу и активирована в режиме роуминга. Однако счета за оказанные услуги связи будут выставлены владельцу, на которого она зарегистрирована.

Для защиты от подобного вида мошенничества никогда не следует передавать свою SIM-карту третьим лицам, особенно незнакомым. При сдаче телефона или другого устройства связи в ремонт необходимо извлечь SIM-карту.

В случае утери (кражи) телефона (SIM-карты) необходимо незамедлительно обратиться к своему оператору сотовой связи для оказания услуг по ее блокировке. Особенно следует придерживаться данных рекомендаций в случае утери телефона за границей во избежание начисления задолженности на большую сумму (при использовании телефона злоумышленниками), которую придется внести по возвращении в Республику Беларусь. Стоит учитывать и тот факт, что счета за пользование мобильной связью в режиме роуминга выставляются оператором пользователям не сразу, а по прошествии достаточного количества времени.

2. Просьба о помощи.

Достаточно распространенный вид мошенничества. Абоненту приходит SMS с просьбой о помощи. Вариантов таких сообщений достаточно много, но суть у них одна. Например: «Мама (папа, сестра, брат и т.д.), пишу с чужого номера. На моем телефоне закончились деньги. Срочно положи столько-то рублей на номер…» Могут приходить сообщения о «попадании в аварию», «неприятности с контролерами в общественном транспорте» и т.д.

Для защиты от такого вида мошенничества всегда необходимо уточнить у родных, друзей, знакомых полученную информацию.

При желании перезвонить на номер, с которого пришло подобное SMS, стоит обратить на него внимание. Так как это может быть короткий номер или номер иностранного оператора.

3. Ошибочный платеж («Верните деньги!»).

Существует несколько схем такого мошенничества, рассмотрим их подробнее.

SMS может приходить как от оператора сотовой связи (злоумышленник на самом деле пополнил баланс мобильного телефона пользователя), так и с произвольного номера, повторяя «оригинальное» сообщение оператора. Причем в первом случае деньги, как правило, зачисляются на счет абонента, а во втором – нет.

Далее на мобильный номер абонента может поступить звонок с просьбой о возврате денежных средств на определенный номер злоумышленника за ошибочно произведенный платеж. Абонент, подтвердив свое согласие о возврате денежных средств, переводит указанную «ошибочную» сумму на мобильный номер злоумышленника. В первом случае злоумышленник обращается с заявлением к сотовому оператору и повторно переводит со счета абонента-жертвы сумму «ошибочного» платежа.

Второй вариант развития событий предполагает, что деньги на счет абонента фактически не поступают, а абонент делится со злоумышленником своими деньгами.

В целях защиты от такого вида мошенничества необходимо помнить, что у всех операторов существует отработанная процедура возврата ошибочно уплаченных средств для пополнения баланса чужого абонентского номера.

В случае возникновения подобной ситуации не стоит переводить денежные средства на незнакомый абонентский номер, а рекомендуется посоветовать звонящему обратиться к оператору сотовой связи в целях урегулирования данного вопроса.

4. Входящие звонки с неизвестных иностранных номеров.

Данный вид мошенничества также основывается на невнимательности абонента.

Например, глубокой ночью абоненту поступает входящий звонок из-за границы, который буквально сразу сбрасывается, а абонент не успевает на него ответить. Абонент, находясь в сонном состоянии, перезванивает на неотвеченный неизвестный иностранный номер, а после установления соединения либо ничего не слышит, либо у него включается автоответчик. При этом со счета абонента списываются денежные средства.

Для защиты от данного вида мошенничества абоненту необходимо проверять номер мобильного оператора, на который он собирается сделать звонок, и без необходимости не перезванивать на незнакомые иностранные номера.

5. Странные номера входящих вызовов и SMS.

Этот вид мошенничества предполагает деятельность злоумышленников, связанную с незаконной терминацией (оригинацией) голосового трафика в обход надлежащих коммутационных узлов операторов электросвязи, уполномоченных на пропуск международного и (или) межсетевого трафика, и (или) использованием услуги IP-телефонии в нарушение установленного законодательством порядка.

Подобная деятельность влечет негативные экономические последствия как для операторов электросвязи, уполномоченных на пропуск международного и (или) межсетевого трафика, а также на оказание услуг телефонии по IP-протоколу в пределах действия сетей электросвязи Республики Беларусь, так и для абонента, с лицевого счета которого в случае осуществления звонка на подобные номера будут списаны средства как за исходящий вызов.

В целях осуществления противодействия такому виду мошенничества абонент может обратиться к своему оператору сотовой связи и сообщить о подобном факте. Оператор электросвязи, совершив необходимые действия, сможет пресечь на стороне своей сети незаконную деятельность третьих лиц.

6. Звонки со стороны «службы поддержки» сотового оператора.

Злоумышленники представляются сотрудниками технической поддержки оператора и под различными предлогами (несвоевременная оплата счета, технические проблемы, случайная блокировка абонентского номера технической службой, сбой в работе оборудования, перевод оборудования оператора для работы с другими голосовыми кодеками и т.д.) предлагают абоненту либо перевести деньги на указанный ими номер, либо оплатить штраф, либо перезвонить на короткий номер для решения возникшей проблемы или на номер телефона, на котором будет включен автоответчик с «рекомендацией», какие действия предпринять абоненту в дальнейшем.

Чтобы исключить данной вид мошенничества, необходимо помнить, что операторы сотовой связи всегда приглашают абонента в фирменный центр продаж своих услуг в целях решения всех возникших проблемных вопросов.

7. Выигрыш приза.

На телефон абонента поступает звонок (также возможно получение SMS). При этом звонящий представляется сотрудником известной радиостанции, банка, телеканала или туристической фирмы и поздравляет абонента с выигрышем ценного приза, туристической поездки и т.д.

Для получения приза абоненту предлагается в течение ближайших минут перезвонить на короткий номер указанной компании, где абонента в очередной раз поздравят с выигрышем ценного приза и предложат оплатить, например, налог на выигрыш, перечислив денежные средства на электронный кошелек или предоставив в течение часа сотруднику компании данные карты экспресс-оплаты за услуги связи на определенную сумму.

После этого обманутый абонент приезжает за призом в офис известной компании и узнает, что никакого розыгрыша не проводилось.

Чтобы не стать жертвой такого мошенничества, не стоит спешить перезванивать на короткие номера и отправлять денежные суммы на электронные кошельки различных платежных систем. Самый верный способ – обратиться в офис названной компании, телеканала, радиостанции, банка или туристической фирмы и на месте уточнить у сотрудников все вопросы, связанные с возможным выигрышем. Не стоит забывать, что, как правило, компании всегда освещают в средствах массовой информации ход и результаты проведения различного рода розыгрышей и акций.

8. Звонки со стороны «банковских структур и организаций».

Всегда стоит помнить, что настоящий технический специалист или сотрудник банка никогда, ни в каких случаях не будет запрашивать у клиента конфиденциальную информацию, касающуюся реквизитов банковской карты, а также персональные данные из паспорта и т.д.

В случае возникновения подозрения, что с вами разговаривает злоумышленник, необходимо прекратить разговор, а для уточнения вопросов, возникших с вашей банковской картой или банковским счетом, самостоятельно перезвонить по номеру горячей линии банка, указанного на его официальном интернет-сайте.

Также не следует перезванивать на тот номер телефона, с которого вам звонили злоумышленники. Так как он с высокой степенью вероятности будет изначально подменен или вы сами можете дозвониться до злоумышленников, которые затем продолжат разыгрывать свой «спектакль».

Стоит в том числе иметь в виду, что в настоящее время существуют технологии, позволяющие злоумышленникам заблокировать телефонную линию жертвы и перенаправлять все последующие ее звонки на мошенников.

В данном случае, если у вас имеются достаточные подозрения, то для связи с банком воспользуйтесь, к примеру, стационарным телефоном.

Запомните, ни в коем случае не сообщайте злоумышленникам реквизиты вашей банковской карты и не осуществляйте перевод средств на другие счета, которые предложены звонящим злоумышленником.»

9. К вам пришла SMS с просьбой перейти по указанной ссылке для разблокирования вашей электронной почты, аккаунта в соцсети и т.д.

SMS-рассылка в настоящее время стала очень популярным инструментом для продвижения своих товаров, работ и услуг, а также информирования клиентов о новых акциях и т.д.

К SMS, которые содержат ссылку, следует относиться с настороженностью. Учитывая, что объем SMS ограничен, многие компании используют сервисы по сокращению ссылок и понять, на какой интернет-ресурс ведет конкретная ссылка, не представляется возможным.

Этим и пользуются злоумышленники, перенаправляя при помощи таких SMS, содержащих сокращенные ссылки, на свои ресурсы, где обычно на визуально схожей с оригинальной страницей интернет-ресурса злоумышленники предлагают, к примеру, ввести свой логин и пароль или иные данные, которые затем получают злоумышленники для доступа к вашему личному кабинету, странице соцсети и т.д.

Кроме того, переход по ссылке может означать автоматический акцепт предлагаемой услуги.

Перед переходом по ссылке, присланной в SMS, всегда следует еще раз перепроверить информацию, позвонив на горячую линию сервиса или зайдя на их интернет-ресурс.

Стоит помнить, что мошенники идут в ногу со временем, а общество постоянно повышает уровень своих цифровых знаний, всё больше узнает о социальной инженерии и иных методах злоумышленников, поэтому используемые сейчас последними способы и средства для хищения денежных средств в скором времени могут стать неактуальными, поэтому в любой ситуации нужно оставаться предельно внимательными и досконально разобраться в случившемся, прежде чем сообщить кому-то свои персональные данные или совершить какие-либо действия по указанию мошенника. Ведь Ваша безопасность, в первую очередь, в Ваших руках!