Профилактика киберпреступлений

Повсеместное внедрение и использование компьютерных информационных технологий, безусловно, создает возможности для более эффективного развития экономики, политики, общества и государства в целом. Однако совершенствование и применение высоких технологий приводит не только к укреплению информационного общества, но и появлению новых угроз, одной из которых является компьютерная преступность.

Экспоненциально увеличивающийся поток информации и преобладание цифровой информации в образовательной среде современной школы актуализируют проблему профилактики цифровой безопасности современных школьников. Особое место в данном вопросе принадлежит профилактике цифровой зависимости школьников, поскольку дети проводят в интернете довольно много времени.

Как известно, интернет не только содержит множество полезной информации и предоставляет выбор развлечений, но и таит массу угроз, которые могут повлиять и на материальное состояние семьи, и на психологическое здоровье детей.

На текущий момент возраст интернет-пользователя снизился настолько, что порой пятилетние малыши обращаются с компьютером и мобильными устройствами более ловко, чем взрослые. Помимо всех известных положительных моментов, интернет несет в себе опасность, которая может затронуть даже пользователей младшего дошкольного возраста.

Рассмотрим основные угрозы, которым подвергается молодежь в современном киберпространстве.

1. ВИШИНГ

Вишинг – один из методов мошенничества с использованием социальной инженерии. Он заключается в том, что злоумышленники, используя телефонную связь и выдавая себя за сотрудников банков (или правоохранителей, что особенно часто происходит в последнее время), под различными предлогами выясняют у потерпевших сведения о наличии банковских платежных карточек (далее – БПК), сроках их действия, CVV (CVC)-кодах, паспортных данных, смс-кодах с целью хищения денежных средств. В ряде случаев злоумышленникам известны некоторые реквизиты БПК, а также анкетные данные лиц, на имя которых они эмитированы.

В большинстве случаев при совершении звонков потерпевшим преступники используют IP-телефонию, которая позволяет маскировать телефонные номера под номера белорусских операторов связи. Кроме этого, зачастую злоумышленники используют мессенджеры Viber и WhatsApp, в которых существует возможность использования

виртуальных номеров. Также преступники маскируются под логотипом узнаваемых белорусских банков, вводя в заблуждение потенциальных жертв.

Злоумышленники звонят жертве и от имени банковского сотрудника сообщают, что необходимо осуществить какие-либо действия с БПК, так как кто-то либо пытается похитить с нее денежные средства, либо оформляет кредит, либо производит подозрительную оплату. Завладев реквизитами карты, преступники осуществляют хищение денежных средств с банковского счета потерпевшего.

В последнее время наиболее актуальная схема – побуждение жертвы открыть кредит. Злоумышленники сообщают жертве о том, что якобы кто-то посторонний пытается открыть кредит на ее имя, и для его деактивации необходимо самостоятельно обратиться в банк и открыть кредит, переслав впоследствии реквизиты счета.

2. ФИШИНГ

Фи́шинг – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям. Фишинг используется для получения доступа к учетным записям пользователей самых различных ресурсов, но зачастую он применяется для хищения данных пользователей торговых онлайн-площадок.

Для этого злоумышленники подменяют страницу используемого жертвой интернет-сервиса на мошенническую, которая внешне является двойником оригинала. Фишинговая страница может иметь сходство с разными сервисами: Kufar, Белпочта, службой доставки, банками, ЕРИП и т.д. В соответствии с этим может использоваться разный предлог для перехода на страницу преступником (забрать зачисленные им деньги, подтвердить получение посылки на почте или в службе доставки, подтвердить прием средств на одном из банковских сервисов и т.д.). Невнимательный интернет-пользователь может и не заметить подмены, так как подобные страницы визуально схожи с оформлением оригинальных сайтов. Когда пользователь заходит на такую поддельную страницу и вводит логин и пароль, они становятся доступны мошенникам.

Стоит отметить, что применяемая злоумышленниками схема хищений характерна не только для Беларуси. Столь же системно эти преступления совершаются в отношении пользователей схожих ресурсов, ориентированных на иные государства СНГ: России (avito.ru), Украины (olx.ua), Казахстана (olx.kz) и др.

3. СВАТИНГ

Сватинг – заведомо ложный вызов полиции, аварийно-спасательных служб, путем фальшивых ложных сообщений об опасности (например, о минировании, убийствах, захвате заложников).

Сватинг в первую очередь распространен в среде, где люди, чаще всего молодые, объединяются по каким-то целям. Например, в онлайн-играх. У них есть термин «вызвать милицию на дом» – когда для того, чтобы, к примеру, досадить обидчику, ему на дом вызывают правоохранителей, либо сообщают о минировании какого-либо объекта.

В последние годы сватинг из забавы любителей онлайн-игр и хакеров превратился в массовое явление и большую проблему для правоохранительных органов различных стран. Общественная опасность таких деяний состоит в том, что заведомо недостоверные сведения дезорганизуют нормальную работу объектов транспорта, предприятий, государственных органов и учреждений, организаций независимо от формы собственности. В свою очередь, это причиняет существенный экономический вред как субъектам хозяйствования, так и гражданам. При этом информация о возможном взрыве, поджоге либо иных действиях, предполагающих тяжкие последствия, способна посеять панику среди населения и внести неудобства в повседневную жизнь.

Стоит отметить, что ответственность за это преступление наступает с 14 лет. Наказание – штраф, арест, ограничение свободы на срок до пяти лет или лишение свободы на срок до семи лет. Если ребенку, сообщившему о ложном минировании, не исполнилось 14 лет, наступает административная ответственность родителей, а ребенка ставят на учет в инспекцию по делам несовершеннолетних.

4. ДДОС-атаки

DoS – это атака на вычислительную систему с целью довести её до отказа, то есть создание таких условий, при которых добросовестные пользователи системы не могут получить доступ к предоставляемым системным ресурсам (серверам), либо этот доступ затруднен. В настоящее время DoS и DDoS-атаки популярны тем, что позволяют довести до отказа практически любую систему.

Обычно атака организуется при помощи троянских программ. Предварительно трояны заражают недостаточно защищенные компьютеры обычных пользователей и могут довольно долгое время никак себя не проявлять на зараженном компьютере, ожидая команды от своего хозяина. Компьютер может подвергнуться такой атаке при посещении различных зараженных сайтов, при получении электронной почты или при установке нелицензионного программного обеспечения. Когда злоумышленник собирается начать атаку, он дает команду, и все ранее зараженные компьютеры начинают одновременно слать запросы на сайт-жертву.

Наиболее массовая DoS-атака в Беларуси была произведена экстремистскими каналами в 2021 году. Злоумышленники, намеренно утаивая информацию об уголовной ответственности за участие в DoS-атаке, привлекли к участию в ней более 10 тысяч граждан

(преимущественно из числа молодежи). Практически все участники этого противоправного действия были установлены, а наиболее активные из них были привлечены к уголовной ответственности.

5. ГРУМИНГ

Груминг – это вхождение взрослого человека в доверие к ребенку с целью сексуального самоудовлетворения. Злоумышленник дистанционно нащупывает связь с ребенком через социальные сети, мессенджеры, онлайн-игры, электронную почту. Затем может вынудить ребенка прислать фотографии интимного характера, вовлечь в изготовление порнографических материалов, склонить к интимной встрече в реальности.

От груминга отличают секстинг — это пересылка личных фотографий, сообщений интимного содержания посредством современных средств связи: сотовых телефонов, электронной почты, социальных интернет-сетей.

Порой под влиянием ситуации или эмоций, может показаться, что переслать такие фото – хорошая идея. Чаще всего парни и девушки делают это флиртуя, поддавшись настойчивым уговорам, пытаясь развлечь своих друзей, чтобы получить их признание (чаще пересылают чужие фото, чтобы похвастаться), или же просто отомстить. Эта идея, прямо скажем, не очень хорошая: злоумышленник может воспользоваться такой доверчивостью во вред.

6. КИБЕРБУЛЛИНГ

Кибербуллинг – травля пользователя через все каналы сетевого общения: социальные сети, форумы, чаты, мессенджеры. Проводить травлю могут как одноклассники, интернет-друзья и т.д., так и совершенно посторонние люди.

Эта форма психологического террора может принимать разные обличия: оскорбления через личные сообщения, публикация и распространение конфиденциальной, провокационной информации о жертве; физическая агрессия и так далее. Причины кибербуллинга: чувство превосходства, зависть, чувство превосходства над соперником, чувство собственной неполноценности, самореализация.

Особо следует отметить способ воздействия запрещенным контентом. Ребенку могут показывать порнографические материалы, нанося ущерб психике, так как изображенное со временем перестанет восприниматься ребенком как аморальное поведение.

Угроза нового времени – так называемые группы смерти. И хотя обычно создателями таких групп являются сами подростки (цель – «хайп», жажда острых ощущений, желание доминировать и управлять другими), в подобных группах создается благоприятствующая атмосфера для культивирования суицидальных намерений.

7. МОШЕННИЧЕСТВО В СОЦСЕТЯХ

В настоящее время особо актуальной становится проблема защиты аккаунтов в социальных сетях и противодействия различным формам и видам мошенничества. Наиболее типичные способы обмана в соцсетях сегодня таковы:

Предоплата

Злоумышленники размещают объявления о продаже каких-либо товаров по бросовым ценам, но для его получения (якобы посредством почтовой пересылки или службы доставки) требуется перечисление предоплаты или задатка на указанные «продавцом» банковскую карту, электронный кошелек. Обычно после перечисления ожидаемый товар так и не поступает, а «продавец» перестает выходить на связь.

Шантаж и вымогательство

В некоторых случаях злоумышленники могут угрожать разглашением различных компрометирующих сведений с целью вымогательства.

Социальные сети – это кладезь персональной информации о человеке. Получив несанкционированный доступ к страницам в социальных сетях, переписке электронных почтовых ящиков и облачным аккаунтам и завладев изображениями, не предназначенными для публичного просмотра, преступники вступают в переписку с потерпевшими, требуя разные денежные суммы и угрожая в случае отказа распространить их в интернете.

Онлайн-игры

Индустрия производства игр для персональных компьютеров и мобильных гаджетов давно стало высокодоходным бизнесом. Не удивительно, что повышенным вниманием она пользуется и у мошенников. Ценность тут представляют и аккаунты пользователей, к которым нередко привязаны реквизиты БПК для покупки игровых преимуществ, и коллекционные предметы, которые игроки также нередко приобретают за реальные деньги.

8. СОВЕТЫ ПО БЕЗОПАСНОСТИ

Существенную часть своей жизни современные дети и подростки проводят в интернете, а значит без базовых знаний в области кибербезопасности им, как и взрослым, не обойтись. Чем раньше начать прививать навыки безопасного взаимодействия с виртуальной средой, тем прочнее они усвоятся. И станут такими же естественными, как мытье рук.

Советоваться с родителями

Если ребенок хочет зарегистрироваться на каком-либо сайте, создать профиль в социальной сети и выложить свои фотографии, лучше перед этим посоветоваться с родителями. Взрослый человек сможет лучше проанализировать ситуацию и понять, опасен ли сайт, а также помочь выбрать снимки, которые можно выложить на всеобщее обозрение.

Установить дистанционный контроль

Функция **«родительского контроля»** – это и как специализированное ПО, так и услуги провайдера, которые включает в себя стандартный набор функций. А именно:

- ограничение времени нахождения ребенка в сети;
- ограничение времени пользования компьютером;
- возможность создания графика с допустимыми часами работы в течение дня;
- блокировка сайтов с запрещенным контентом;
- ограничение на запуск приложений (например, игр и иных приложений) и установку новых программ.

Беречь личные данные

Даже если ребенок думает, что хорошо знает человека, с которым общается онлайн, не нужно рассказывать подробности о себе и о родителях. Номер телефона, адрес, номер школы и класса, место работы родителей и их график, время, когда в квартире нет взрослых, а также данные из документов, номера банковских карт – такую информацию ни в коем случае нельзя передавать другим людям.

Не делиться информацией о знакомых

Правило, приведенное выше, распространяется и на других людей. Не нужно рассказывать про друзей и одноклассников, сообщать, где они живут и учатся, какие кружки посещают. Нельзя показывать их фотографии – ни выкладывать их в своих профилях в социальных сетях, ни тем более в частной переписке.

Если хочется выложить групповое фото с праздника или тренировки, сначала стоит обсудить это с теми, кто изображен на снимке. И лучше, если они сообщат родителям, что такое фото публикуется в интернете.

Фильтровать информацию

Мошенники активно используют интернет в своих интересах. Они могут обманывать людей и манипулировать ими, давя на жалость или страх. Поэтому надо научиться скептически относиться к любой информации, размещенной в интернете, и не доверять слепо всему, что там пишут.

Администрация Московского района г. Бреста

ОСТОРОЖНО!
МОШЕННИКИ В ИНТЕРНЕТЕ

НЕ следуй инструкциям незнакомцев, позвонившим с неизвестного номера

НЕ сообщай неизвестным лицам свои персональные данные

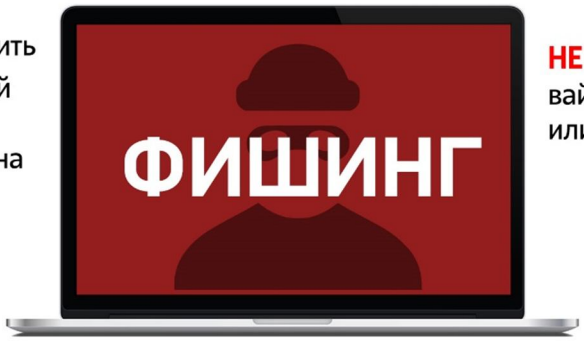
НЕ совершай никаких действий на смартфоне по просьбе посторонних лиц

НЕ переводи деньги незнакомым людям в качестве предоплаты

Сохрани эту информацию и поделись с другими

ОСТОРОЖНО!
МОШЕННИКИ В ИНТЕРНЕТЕ

Не торопись переходить по ссылке, полученной от незнакомца: возможно, она ведет на фишинговый сайт



НЕ пользуйся открытыми вай-фай-сетями в кафе или на улице

Не спеши переходить по ссылке: введи адрес вручную

Фишинговая ссылка может прийти в мессенджере, по электронной почте, в смс-сообщении

Сохрани эту информацию и поделись с другими

ВНИМАНИЕ!

БЕЗОПАСНОЕ ИСПОЛЬЗОВАНИЕ СОЦСЕТЕЙ, МЕССЕНДЖЕРОВ И ЭЛЕКТРОННОЙ ПОЧТЫ!

НЕЛЬЗЯ

Размещать персональную и контактную информацию о себе в открытом доступе

Использовать указание геолокации на фото в постах

Отвечать на агрессию и обидные выражения

Реагировать на письма от неизвестного отправителя

Открывать подозрительное вложение к письму

Сохрани эту информацию и поделись с другими

ВНИМАНИЕ!

ЗАЩИТИ СВОЮ БАНКОВСКУЮ КАРТУ

НЕЛЬЗЯ

Хранить пинкод вместе с картой

Распространять личные данные, логин и пароль доступа к системе «Интернет-банкинг»

Сообщать CVV-код или отправлять его фото

Сообщать данные, полученные в виде SMS-сообщений, сеансовые пароли, код авторизации и т.д.

Сохрани эту информацию и поделись с другими

ВНИМАНИЕ!

ЦИФРОВАЯ БЕЗОПАСНОСТЬ В ИНТЕРНЕТЕ

НЕ переходите по ссылкам и письмам от незнакомцев, не нажимайте на картинки и кнопки

УСТАНОВИТЕ АНТИВИРУС НА ВСЕ ВАШИ УСТРОЙСТВА

НЕ сообщайте свои персональные данные и данные банковской карты

НЕ верьте обещаниям внезапных выигрышей

НЕ используйте одинаковые пароли для всех аккаунтов

НЕ указывайте личную информацию в открытых источниках

Сохрани эту информацию и поделись с другими

ВНИМАНИЕ!
АТАКА НА ГОСОРГАНИЗАЦИИ!

СПЕЦИАЛИСТЫ ОТМЕЧАЮТ УВЕЛИЧЕНИЕ ЧИСЛА ФИШИНГОВЫХ АТАК НА ЭЛЕКТРОННЫЕ ПОЧТОВЫЕ ЯЩИКИ ГОСОРГАНИЗАЦИЙ!

ПРИ РАБОТЕ С ЭЛЕКТРОННОЙ ПОЧТОЙ

НЕ НАДО:

... ОТКРЫВАТЬ ВЛОЖЕНИЯ ПОЧТОВЫХ СООБЩЕНИЙ ОТ НЕИЗВЕСТНЫХ ОТПРАВИТЕЛЕЙ

... ПЕРЕХОДИТЬ ПО ССЫЛКАМ, ПОЛУЧЕННЫМ ОТ НЕИЗВЕСТНЫХ

... ХРАНИТЬ И ПЕРЕДАВАТЬ В ОТКРЫТОМ ВИДЕ ВАЖНЫЕ ДАННЫЕ (ЗААРХИВИРУЙТЕ ИХ И УСТАНОВИТЕ ПАРОЛЬ)

... ПРИ РЕГИСТРАЦИИ ЯЩИКА УКАЗЫВАТЬ БИОГРАФИЧЕСКИЕ ДАННЫЕ, ИСПОЛЬЗОВАТЬ ПРОСТЫЕ ПАРОЛИ И ПОВТОРЯЮЩИЕСЯ СИМВОЛЫ

НАДО:

... ПОДКЛЮЧИТЬ 2-ФАКТОРНУЮ АУТЕНТИФИКАЦИЮ

... РЕГУЛЯРНО МЕНЯТЬ ПАРОЛЬ ОТ ЭЛ.ПОЧТЫ

... ИСПОЛЬЗОВАТЬ НЕСКОЛЬКО ПОЧТОВЫХ ЯЩИКОВ ДЛЯ РАЗНЫХ РЕСУРСОВ (ПЕРЕПИСКА, РЕГИСТРАЦИЯ, ДЕЛОВАЯ ПОЧТА)

... ИСПОЛЬЗОВАТЬ УНИКАЛЬНЫЕ ПАРОЛИ ДЛЯ РАЗНЫХ ИНТЕРНЕТ-РЕСУРСОВ

... ВВОДИТЬ ИНФОРМАЦИЮ ТОЛЬКО НА ЗАЩИЩЕННЫХ САЙТАХ (HTTPS)

ВНИМАНИЕ!

ЕДИНСТВЕННЫЙ НАДЕЖНЫЙ СПОСОБ ЗАЩИТЫ – ЭТО ВАША БДИТЕЛЬНОСТЬ!

ГЛАВНОЕ УПРАВЛЕНИЕ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ КМ МВД БЕЛАРУСИ

КАК ЗАЩИТИТЬ ПРЕДПРИЯТИЕ ОТ КИБЕРУГРОЗ

В 2018-2020 ГГ ПРЕДПРИЯТИЯМ ПРИЧИНЕН УЩЕРБ НА СУММУ БОЛЕЕ 2 МЛН. РУБЛЕЙ

ОСНОВНЫЕ СХЕМЫ КИБЕРПРЕСТУПНИКОВ

Шифрование коммерческой информации

Хакеры получают доступ к данным организации, превращают их в бессмысленный набор символов и оставляют письмо с предложением расшифровать данные за деньги.

Подмена реквизитов для перевода средств

Эта криминальная схема используется в длительных и успешных деловых отношениях белорусской фирмы и зарубежного контрагента, которые активно контактируют по электронной почте. Злоумышленники получают доступ к одному из ящиков, участвующих в переписке. Когда у компаний намечается крупная сделка, со взломанного email предприятия (или же другой электронной почты с максимально похожим адресом) хакеры высылают письмо, в котором от имени юрлица уведомляют партнеров об изменении реквизитов для перевода средств.

Фишинговое письмо

На электронную почту учреждения приходит письмо с вложением-вредоносом, способным превращать ценную для компании информацию в бесполезный набор символов.

КАК ЗАЩИТИТЬСЯ ОТ КИБЕРУГРОЗ

воспользоваться услугами профессионалов по защите данных

регулярно выполнять резервное копирование данных

пользоваться актуальными антивирусами

настроить специальное программное обеспечение, блокирующее таргетированные атаки на информационные системы

ГЛАВНОЕ УПРАВЛЕНИЕ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ КМ МВД РБ

Как не стать жертвой киберпреступника.

ЗАЩИТА БАНКОВСКОЙ КАРТОЧКИ

Основные правила информационной безопасности по защите банковской карточки:

- хранить в тайне пин-код карты
- прикрывать ладонью клавиатуру при вводе пин-кода
- оформлять отдельную карту для онлайн-покупок
- деньги зачислять только в размере предполагаемой покупки
- использовать услугу 3-D Secure* и лимиты на максимальные суммы онлайн-операций
- скрыть CVV-код** на карте (трехзначный номер на обратной стороне), предварительно сохранив его
- подключить услугу "SMS-оповещение"

Не рекомендуется

- хранить пин-код вместе с карточкой/на карточке
- сообщать CVV-код или отправлять его фото
- распространять личные данные (например паспортные), логин и пароль доступа к системе "Интернет-банкинг"
- сообщать данные, полученные в виде SMS-сообщений, сеансовые пароли***, код авторизации, пароли 3-D Secure

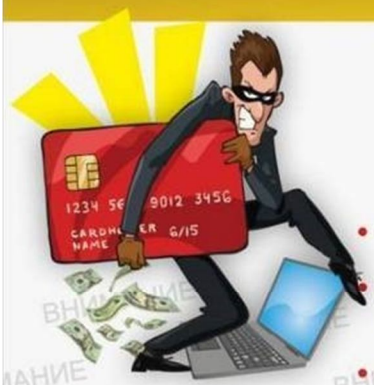
** Услуга 3-D Secure - для подтверждения онлайн-платежа держатель карточки вводит особый код (получает его в смс-сообщении на телефон).*

*** Код CVV - последние 3 цифры номера на обратной стороне платежной карты справа на белой линии, предназначенной для подписи. Код дает возможность распоряжаться средствами, находящимися на счету, физически не контактируя с картой.*

**** Сеансовый пароль - предоставляется при входе в интернет-банкинг, действителен лишь в течение одного платежного сеанса.*

Источник: МВД Беларуси.

ВНИМАНИЕ! УЧАСТИЛИСЬ СЛУЧАИ ТЕЛЕФОННОГО МОШЕННИЧЕСТВА!



ОН МОЖЕТ ПОПРОСИТЬ:

МОШЕННИК МОЖЕТ ПРЕДСТАВИТЬСЯ:

- Сотрудником Банка
- Сотрудником службы безопасности банка
- Сотрудником больницы
- Сотрудником благотворительной организации
- Родственником

И НЕ ВЕДИТЕСЬ НА НА СЛОВА!!! МОШЕННИКА:

- Ваша карта заблокирована
- В отношении вашей карты предпринимаются мошеннические действия
- Вашему родственнику нужна помощь или лечение
- Вам положена отсрочка по кредиту или пособию

Данные карты:

- номер карты
- CVV/CVC-код
- PIN-код
- срок действия карты

Пароль:

- от интернет-банка;
- из SMS-сообщения *(для входа в интернет-банк или подтверждения операции)*

Перевести деньги:

- на специальный счет или карту, где они будут в безопасности

НЕ

- сообщайте никому данные карты
- сообщайте никому пароли и коды из SMS
- выполняйте действия с банковской картой по просьбе третьих лиц

МОШЕННИЧЕСКАЯ СХЕМА “ЧЕЛОВЕК ПОСЕРЕДИНЕ”:
ЗАЩИТИТЕ СВОЮ ЭЛЕКТРОННУЮ ПОЧТУ!

НИКОМУ НЕ СООБЩАЙТЕ ПАРОЛИ, НЕ ИСПОЛЬЗУЙТЕ АВТОСОХРАНЕНИЕ В БРАУЗЕРЕ

ПРОВЕРЯЙТЕ ПРАВИЛЬНОСТЬ АДРЕСА КОНТРАГЕНТА

НЕ ИСПОЛЬЗУЙТЕ В ЛИЧНЫХ ЦЕЛЯХ СЛУЖЕБНЫЕ ЭЛ.ЯЩИКИ

ПРЕЖДЕ, ЧЕМ ОТПРАВИТЬ ПЕРЕВОД, СОЗВОНИТЕСЬ С ПОЛУЧАТЕЛЕМ

ГЛАВНОЕ УПРАВЛЕНИЕ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ КМ МВД БЕЛАРУСИ

Как не стать жертвой киберпреступника.
ЗАЩИТА БАНКОВСКОЙ КАРТЫ

Наиболее распространенные методы работы злоумышленников

выманивание реквизитов банковских платежных карт с использованием взломанных аккаунтов знакомых в социальных сетях

ЛЖЕПОКУПАТЕЛЬ - под видом покупателя злоумышленник связывается с продавцом, предлагает внести залог перед покупкой товара, а для получения денежного перевода предоставляет ему ссылку на мошеннический сайт, визуально похожий на официальный сайт банка

ВИШИНГ - представляясь по телефону сотрудником банка, злоумышленник пытается узнать у держателя карты конфиденциальную информацию (ее реквизиты, а также номер паспорта, личный идентификационный номер, логины, пароли, СМС-коды)

НЕ СООБЩАЙТЕ НИКОМУ

- информацию, размещенную на вашей банковской платежной карте (на обеих сторонах): номер, дату, код
- цифровые или буквенные коды
- паспортные данные

ЕСЛИ ВАМ ПОСТУПИЛ СОМНИТЕЛЬНЫЙ ЗВОНОК

- немедленно завершите разговор
- обратитесь в контакт-центр банка, выпустившего карту
- следуйте рекомендациям сотрудника банка

Для защиты денежных средств клиентов у банка есть вся необходимая информация

Работники банка по телефону не должны спрашивать ни реквизиты карты, ни паспортные данные

Не давайте никому свой мобильный телефон и предупредите об этом ваших близких, особенно детей и лиц пожилого возраста

Источник: Национальный банк Беларуси.

ВНИМАНИЕ!

БЕРЕГИТЕ СВОИ ДЕНЬГИ!

УЧАСТИЛИСЬ СЛУЧАИ ХИЩЕНИЯ ДЕНЕГ С БАНКОВСКИХ КАРТ-СЧЕТОВ!

Если вам пришло сообщение в мессенджере, социальных сетях или по электронной почте...

... в котором говорится, что банковская карта заблокирована, и предлагается разблокировать ее, пройдя по ссылке...

... ни в коем случае не переходите по ссылке! Незамедлительно обращайтесь в службу безопасности банка!

Если вы получили сообщение о блокировке банковской карты:

- не переходите по прикрепленной ссылке, никуда не пересылайте свои данные;
- проверьте баланс своей карты в банкомате, инфокиоске, мобильном или интернет-банкинге;
- обратитесь в службу безопасности банка.

Главное управление по противодействию киберпреступности криминальной милиции МВД Республики Беларусь

ГЛАВНЫЕ ПРАВИЛА ЦИФРОВОЙ ГИГИЕНЫ ДЛЯ ДЕТЕЙ

Не сообщай личную информацию незнакомцу. И, вообще, в интернете не размещай сведения о себе и семье

Советуйся с родителями, как правильно поступить, если столкнулся с чем-то непонятным или пугающим

Помни, что в интернете надо быть очень-очень внимательным. Старайся избегать общения с незнакомыми людьми в онлайн-играх и соцсетях, не выполняй бездумно то, что они попросят тебя сделать

ГЛАВНОЕ УПРАВЛЕНИЕ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ МВД

БЫТЬ ХАКЕРОМ:

НЕ РАЗВЛЕЧЕНИЕ, А ПРЕСТУПЛЕНИЕ!

УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ ЗА КИБЕРПРЕСТУПЛЕНИЯ НАСТУПАЕТ:

С 14 ЛЕТ

СТАТЬЯ 212 УК БЕЛАРУСИ

ХИЩЕНИЕ ИМУЩЕСТВА ПУТЕМ МОДИФИКАЦИИ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ НАКАЗЫВАЕТСЯ ВПЛОТЬ ДО ЛИШЕНИЯ СВОБОДЫ НА СРОК **до 12 ЛЕТ**

СТАТЬЯ 340 УК БЕЛАРУСИ

ЗАВЕДОМО ЛОЖНОЕ СООБЩЕНИЕ ОБ ОПАСНОСТИ НАКАЗЫВАЕТСЯ ВПЛОТЬ ДО ЛИШЕНИЯ СВОБОДЫ НА СРОК **до 7 ЛЕТ**

С 16 ЛЕТ

СТАТЬЯ 349 УК БЕЛАРУСИ

НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ НАКАЗЫВАЕТСЯ ВПЛОТЬ ДО ЛИШЕНИЯ СВОБОДЫ НА СРОК **до 7 ЛЕТ**

СТАТЬЯ 222 УК БЕЛАРУСИ

НЕЗАКОННЫЙ ОБОРОТ СРЕДСТВ ПЛАТЕЖА И (ИЛИ) ИНСТРУМЕНТОВ НАКАЗЫВАЕТСЯ ВПЛОТЬ ДО ЛИШЕНИЯ СВОБОДЫ НА СРОК **до 10 ЛЕТ**

ВНИМАНИЕ! ОПЕРАЦИЯ «ВИШИНГ»!

АФЕРИСТ МОЖЕТ ПОЗВОНИТЬ ПО ПОВОДУ ТОВАРА НА ТОРГОВОЙ ПЛОЩАДКЕ И ПРЕДЛОЖИТЬ СДЕЛКУ С ПРЕДОПЛАТОЙ

АФЕРИСТ МОЖЕТ ПРЕДСТАВИТЬСЯ БАНКОВСКИМ РАБОТНИКОМ И ВЫМАНИТЬ КОНФИДЕНЦИАЛЬНЫЕ ДАННЫЕ

АФЕРИСТ СООБЩАЕТ, ЧТО РОДСТВЕННИК ЖЕРТВЫ ПОПАЛ В БЕДУ И ЕМУ НУЖНА ФИНАНСОВАЯ ПОМОЩЬ

ВИШИНГ - СПОСОБ МОШЕННИЧЕСТВА С ПОМОЩЬЮ ТЕЛЕФОНА, КОГДА МОШЕННИК ПОД РАЗЛИЧНЫМ ПРЕДЛОГОМ ПЫТАЕТСЯ ВЫМАНИТЬ ПЕРСОНАЛЬНУЮ ИНФОРМАЦИЮ ЖЕРТВЫ ДЛЯ ПОСЛЕДУЮЩЕГО ХИЩЕНИЯ ДЕНЕГ С ЕЕ БАНКОВСКОГО СЧЕТА

- НИКОГДА НЕ СООБЩАЙТЕ НЕЗНАКОМОМУ СВОИ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

- НЕ ТОРОПИТЕСЬ ВЫПОЛНЯТЬ ТО, ЧТО ОТ ВАС ПРОСИТ СОБЕСЕДНИК. МОШЕННИКИ ОЧЕНЬ ИЗОБРЕТАТЕЛЬНЫ И УБЕДИТЕЛЬНЫ!

- НАДЕЖНО ЗАЩИЩАЙТЕ СВОИ ДАННЫЕ (ДВУХФАКТОРНАЯ АВТОРИЗАЦИЯ, СМС-ОПОВЕЩЕНИЕ , И Т.Д.)

- В СЛУЧАЕ УТЕРИ ИЛИ КРАЖИ КАРТЫ ЗАБЛОКИРУЙТЕ ЕЕ ПО ТЕЛЕФОНУ ИЛИ В БАНКЕ

ГУПК КМ МВД РЕСПУБЛИКИ БЕЛАРУСЬ

ВНИМАНИЕ! ОТКРЫТЫЙ WI-FI

УГРОЗА ДЛЯ ВЛАДЕЛЬЦЕВ WI-FI:

- ЗЛОУМЫШЛЕННИК МОЖЕТ ВНЕДРИТЬ ВРЕДОНОСНЫЕ ПРОГРАММЫ НА ВАШЕ УСТРОЙСТВО ЧЕРЕЗ ОТКРЫТОЕ WI-FI-СОЕДИНЕНИЕ

- ВАШ ТРАФИК МОЖЕТ БЫТЬ ПЕРЕХВАЧЕН ЗЛОУМЫШЛЕННИКОМ, ВКЛЮЧАЯ ПЕРСОНАЛЬНЫЕ ДАННЫЕ, РЕКВИЗИТЫ КАРТ, И Т.Д.

- ВАШ КОМПЬЮТЕР МОЖЕТ БЫТЬ ПОДКЛЮЧЕН К БОТ-СЕТИ, ОСУЩЕСТВЛЯЮЩЕЙ DDOS-АТАКИ, ЧТО МОЖЕТ ПОВЛЕЧЬ УГОЛОВНУЮ ОТВЕТСТВЕННОСТЬ

УГРОЗА ДЛЯ ПОЛЬЗОВАТЕЛЕЙ:

- ВВОДИМЫЕ ВАМИ ПЕРСОНАЛЬНЫЕ ДАННЫЕ МОГУТ БЫТЬ ПЕРЕХВАЧЕНЫ ХАКЕРОМ (ПЛАТЕЖНАЯ ИНФОРМАЦИЯ, РЕВИЗИТЫ, КОНТАКТЫ НА ТЕЛЕФОНЕ, ПАРОЛИ)

- ЗЛОУМЫШЛЕННИК МОЖЕТ ПОЛУЧИТЬ ДОСТУП К ВАШИМ ПЕРСОНАЛЬНЫМ ДАННЫМ, ФОТО-ВИДЕО, ХРАНЯЩИМСЯ НА УСТРОЙСТВЕ, И Т.Д.

- ЗЛОУМЫШЛЕННИК МОЖЕТ ВЗЛОМАТЬ ВАШИ ПРОГРАММЫ И СОЦИАЛЬНЫЕ СЕТИ, СОВЕРШАЯ ЗАТЕМ РАЗЛИЧНЫЕ ДЕЙСТВИЯ ОТ ВАШЕГО ИМЕНИ

ГЛАВНОЕ УПРАВЛЕНИЕ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ
КРИМИНАЛЬНОЙ МИЛИЦИИ МВД РЕСПУБЛИКИ БЕЛАРУСЬ

Безопасный интернет для детей

СОХРАНИ ИНФОРМАЦИЮ

- не сообщай незнакомцам свой логин и пароль
- не открывай файлы из непроверенных источников
- не заходи на сайты, которые защита компьютера считает подозрительными

РОДИТЕЛИ! научите детей пользоваться интернетом правильно!

ГЛАВНЫЕ ПРАВИЛА ЦИФРОВОЙ ГИГИЕНЫ

НЕ отправляй незнакомцам свои фото и видео

Злоумышленники могут узнать что-то нужное им о твоей жизни

НЕ встречайся с людьми, с которыми знаком только в интернете

За маской онлайн-собеседника может скрываться злоумышленник

НЕ сообщай в интернете свой реальный адрес и телефон

Злоумышленник может встретить тебя с недобрыми намерениями

НЕ отправляй личные данные для участия в конкурсах на малоизвестных сайтах

Информацией могут завладеть и воспользоваться недоброжелатели

Всегда важно помнить: неправильное поведение в интернете может принести большой вред.

не дай себя обмануть!

МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ
РЕСПУБЛИКИ БЕЛАРУСЬ

круглосуточный единый номер 102

Топ-8 грязных схем

БУДЬТЕ ВНИМАТЕЛЬНЫ!

! ИНТЕРНЕТ-МОШЕННИКОВ

ЗВОНОК ИЗ БАНКА

Звонящий представляется сотрудником службы безопасности банка и уверяет: «С вашей карты кто-то хотел похитить деньги, для отмены операции назовите свои данные». Выманив сведения, мошенник выводит со счета все средства и исчезает.

Как не попасться? Скажите, что вы не клиент этого учреждения (даже если это так). Если на той стороне мгновенно переключат на «специалиста из вашего банка» - это точно мошенничество.

Или просто положите трубку и перезвоните в банк сами. Только номер телефона смотрите не во «Входящих», а на сайте.

СБОР ДЕНЕГ НА ЛЕЧЕНИЕ

Мошенники в соцсетях создают группу якобы с целью сбора средств на лечение тяжелобольного. Деньги предсказуемо забирают себе.

Как не попасться? Запросите у администратора группы справки, документы, другие дополнительные сведения.

ПИСЬМО ОТ ДРУГА

Преступник взламывает чужие соцсети и рассылает друзьям пользователя сообщения с просьбой сбросить денег или отправить откровенные фото. Мошенник заранее изучает переписку жертвы и выбирает максимально похожий стиль письма.

Как не попасться? Позвоните другу и уточните, действительно ли он вам пишет.

Если нет возможности позвонить - напишите в другом мессенджере.

ДЕШЕВЫЕ ВЕЩИ

Вор создает в социальной сети (чаще - в Instagram и «ВКонтакте») страницу якобы интернет-магазина с подозрительно низкими ценами. Когда жертва вносит предоплату или перечисляет всю стоимость товара, то оказывается в «черном списке» и больше не может связаться с продавцом.

Как не попасться? На странице найдите реквизиты продавца (как минимум, УНП, который должен указываться обязательно) и проверьте их на сайте kartoteka.by, поищите отзывы через поисковик.

Настаивайте на отправке с наложенным платежом (оплата при получении).

АРЕНДА КВАРТИР

Выставив низкую цену за аренду квартиры, мошенник ждет откликов. В переписке уверяет: интерес большой, чтобы оставить бронь - внесите предоплату. Дальше два пути: или бросает фейковую страницу и сразу крадет введенные данные карты, или дает реальные реквизиты своего пластика (усыпляет бдительность). Во втором случае будьте готовы получить сообщение об отмене сделки с извинениями и просьбой прислать информацию о счете якобы для возврата средств.

Как не попасться? Настаивайте на личной встрече для передачи денег под расписку.

Еще одна простая проверка - попросить созвониться: фальшивые «арендодатели» под разными предлогами избегают живых разговоров.

ЗАНЯТОЙ ПОКУПАТЕЛЬ

Человек активно интересуется товаром на торговой площадке (том же «Куфаре») и просит либо отправить посылку курьером (тяжело нести с почты/не может отлучиться с работы), либо прямо сейчас принять предоплату на карту. Следом в переписку летит фишинговая ссылка, где нужно указать данные карточки.

Как не попасться? Откажитесь от таких форм оплаты/доставки.

Не вводите данные карты (особенно - срок действия и CVV-код) на сайтах, куда перешли по ссылкам от незнакомцев.

Не соглашайтесь уходить с торговой площадки и продолжать переписку в другом приложении.

РОЗЫГРЫШИ И ЛОТЕРЕИ (=ОТДАМ ДАРОМ)

На почту или в личку приходят письма вроде «Вы сделали репост и выиграли приз!». Или кто-то на сайте-барахолке обещает отдать даром дорогой гаджет. Следом - условия получения: надо указать паспортные данные и заплатить за доставку (страховку).

Как не попасться? Не переходите ни по каким ссылкам из письма (даже если они якобы ведут к результатам игры). Через поисковик узнайте, действительно ли розыгрыш был проведен, есть ли другие призеры.

МНЕ ТОЛЬКО ПОЗВОНИТЬ

Человек просит ваш телефон срочно позвонить кому-то, потому как у него сел аккумулятор. Получив мобильный, мошенник быстро устанавливает на него следящее приложение. Как только вы решите войти в интернет-банкинг, вор перепишет данные и опустошит счет или прямо в личном кабинете возьмет кредит.

Как не попасться? Лучше вовсе не давать свой смартфон кому-то. Или набирайте номер сами и блокируйте экран, когда будете передавать гаджет для разговора.

Интернет-преступлений становится больше!

Словарь

БУДЬТЕ ВНИМАТЕЛЬНЫ!

Фишинг

Это поддельные сообщения-ссылки вроде «Вам поступил денежный перевод», которые приходят на электронную почту (чаще), через СМС или мессенджеры.

Если просто откроете (прочтете) сообщение - ничего страшного. Но как только перейдете по зараженной ссылке внутри письма или введете там персональную информацию - мошенники получат доступ к данным на компьютере или телефоне. Им не составит труда захватить ваши странички в соцсетях, украсть реквизиты банковских карт.

ПЕРЕХОДИТЬ ПО ССЫЛКАМ ИЗ ПОДОЗРИТЕЛЬНЫХ ПЛАТЕЖНЫХ ПИСЕМ НЕЛЬЗЯ

Вишинг

Это прием, когда мошенники выведывают логины/пароли через звонок по телефону. Узнав нужные данные, преступники снимают с карты деньги и исчезают навсегда.

Если посторонний просит CVV-код - он 100% хочет опустошить ваш счет.

СРАЗУ КЛАДИТЕ ТРУБКУ, ЕСЛИ ЗВОНЯЩИЙ ПРОСИТ ЛОГИН/ПАРОЛЬ ОТ ИНТЕРНЕТ-БАНКИНГА ИЛИ ДАННЫЕ ИЗ СМС

Многофакторная (двухэтапная) аутентификация

Это дополнительная защита. То же самое, что второй замок на двери, ключ от которого находится в другой связке.

Если вы включите ее (во вкладках «Настройки», «Конфиденциальность»), то приложение будет просить не один пароль, а два (или даже больше).

Вход в аккаунт станет дольше, но на сегодня это самая работающая защита - убережет от 99% распространенных атак.

ВКЛЮЧИТЕ МНОГОЭТАПНУЮ АУТЕНТИФИКАЦИЮ

Фальшивый сайт

Это интернет-страница, повторяющая оформление настоящей. Вот только данные, которые вы вводите на ней, идут прямиком в руки мошенников.

Визуально заметить подмену сложно, но есть характерные маркеры:

- замочек слева от адресной строки не замкнут или есть надпись «Не защищено»;
- электронный адрес ненастоящий или буквы в нем перепутаны (bel-post.by вместо belpost.by, bealrusbank.by вместо belarusbank.by).

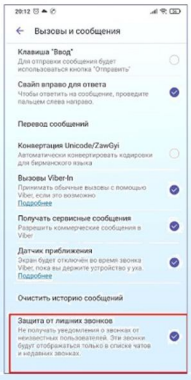
ВНИМАТЕЛЬНО СМОТРИТЕ НА АДРЕСНУЮ СТРОКУ САЙТА

Удаленный доступ

Мошенники просят установить из Google Play или App Store приложение (чаще всего - AnyDesk или TeamViewer, но есть и другие) и с его помощью получают доступ к чужому гаджету. Они смогут увидеть и записать все логины/пароли/коды, которые вы вводите в соцсетях, интернет-банкинге.

ОТКАЖИТЕСЬ, ЕСЛИ НЕЗНАКОМЕЦ ПРОСИТ ВАС УСТАНОВИТЬ КАКОЕ-ЛИБО ПРИЛОЖЕНИЕ

Защита от лишних звонков



Откройте «Вайбер» на телефоне, войдите в раздел «Еще» (правый нижний угол) и выберите вкладку «Настройки». Нажмите на «Вызовы и сообщения» и активируйте пункт «Защита от лишних звонков». Если такой строчки нет - обновите «Вайбер».

Теперь вы не будете получать звонки от неизвестных контактов (они автоматически получат пометку «пропущенный»).

АКТИВИРУЙТЕ ЗАЩИТУ ОТ ЛИШНИХ ЗВОНКОВ СЕБЕ И БЛИЗКИМ

ФИШИНГ: КАК ЗАЩИЩИТЬ СВОЙ БАНКОВСКИЙ СЧЕТ

НИКОГДА НЕ ПЕРЕХОДИТЕ ПО НЕЗНАКОМЫМ ССЫЛКАМ, ПРИСЛАННЫМ ВАМ В МЕССЕНДЖЕРАХ, ПО ЭЛ.ПОЧТЕ, В SMS-СООБЩЕНИИ

Признаки явного мошенничества

Потенциальный покупатель вашего товара предлагает перейти в мессенджер, отказываясь общаться непосредственно на торговой площадке.

Наиболее крупные площадки для защиты своих пользователей ограничивают функцию отправки ссылок

Неизвестный в мессенджере присылает ссылку для перехода на интернет-сайт под предлогом контроля карт-счета, просмотра баланса или проверки состояния оплаты.

Незнакомец предлагает передать ему полные данные вашей банковской карты, включая CVV-код либо логин и пароль от вашего интернет-банкинга.

ПОДРОБНОСТИ - ПО QR-ССЫЛКЕ

ГЛАВНОЕ УПРАВЛЕНИЕ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ КМ МВД РЕСПУБЛИКИ БЕЛАРУСЬ