ИНФОРМАЦИОННЫЕ МАТЕРИАЛЫ ПО ВОПРОСАМ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОСУЩЕСТВЛЕНИЯ ПЛАТЕЖЕЙ В СЕТИ ИНТЕРНЕТ

В настоящее время киберпреступность представляет серьезную угрозу для развития экономики и общества. За последние годы количество киберпреступлений значительно увеличилось, что требует принятия срочных мер для защиты информации и обеспечения кибербезопасности. Одной из основных проблем является недостаточная осведомленность о кибербезопасности среди населения. Многие граждане не принимают достаточных мер предосторожности при использовании сети Интернет, что делает их уязвимыми перед преступниками.

По статистике женщины в 2 раза чаще становятся потерпевшими, чем мужчины. Абсолютное большинство проживает в городах. Люди с высшим в равной степени, как и со средним образованием, подвержены обману. Среди жертв киберпреступников, в основном, экономически активные граждане, представляющие практически все сферы деятельности – бухгалтеры, экономисты, директоры, заместители директоров частных и государственных учреждений, начальники управлений и отделов госучреждений, педагоги, врачи и медсестры, студенты, юристы, программисты и представители других специальностей.

Мошенники регулярно меняют свои схемы обмана граждан, чтобы похитить их деньги. Основными формами обмана являются телефонное и интернет-мошенничество, а также фишинговые ресурсы.

ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО – ВИШИНГ

Мошенники под видом работников банка, операторов связи или государственных органов обращаются к гражданам, создают стрессовую ситуацию, сообщают о проблеме, а потом предлагают помощь в ее решении. При этом чтобы войти в доверие, могут выслать фото служебных документов или даже выйти на видеосвязь в мессенджере.

Распространен способ, когда мошенники, используя различные вымышленные ситуации, убеждают потенциальных жертв загрузить направленный в мессенджере файл или установить **определенное мобильное приложение**. В обоих случаях мошенники получают возможность удаленно управлять устройством, на котором установлено. Таким образом они получают доступ к личным данным пользователей, в том числе имеют возможность оформить онлайн-кредит. Также злоумышленники убеждают **оформить кредиты в банках**, а деньги перевести на «защищенный» счет.

Всегда надо быть начеку и не доверять незнакомым, ни под каким предлогом не устанавливать непроверенные программы и файлы, полученные в мессенджере от неизвестных, не передавать кому бы то ни было деньги и не переводить их на банковские счета по указанию незнакомых.

Мошенники для совершения преступлений изучают свою жертву, собирают в сети Интернет данные о ней и ее интересах, окружении и прочем. Имея образец голоса или фото знакомых, могут создавать фейковые текстовые или видеосообщения.

Мошенники регулярно подбирают новые способы обмана, чтобы получить деньги. В сети Интернет размещают рекламу якобы **инвестиционных платформ**, которых на самом деле не существует, чтобы заманить вкладчиков и похитить их деньги. Первым шагом для связи с куратором является заполнение формы, где необходимо оставить свои имя и телефон. Далее с заинтересовавшимся связывается так называемый куратор, под руководством которого в надежде заработать легкие деньги потенциальная жертва сама переводит деньги на электронный кошелек. Чтобы получить хотя бы вложенные деньги обратно, мошенники требуют заплатить комиссии, взносы и т.д. Некоторое время мошенники рисуют жертве их прибыль, пока у обманутого человека не закончатся деньги, потом связь с ним прекращается. Деньги остаются на мошеннических счетах.

Чтобы не стать жертвой киберпреступника, как можно раньше закончите разговор с неизвестным лицом, кем бы он не представился.

ФЕЙКОВЫЕ МАГАЗИНЫ в соцсетях

Ежедневно в милицию обращаются и те, кто сами перевели **предоплату за товар**, который нашли в объявлениях в социальных сетях и на торговых площадках, и не получили его. Мошенники намеренно создают аккаунты от имени магазинов, в которых размещают объявления несуществующих товаров с заниженными ценами (обувь, одежда, мобильные телефоны, постельное белье, новогодние ели, садовые кресла-качалки-коконы и другие товары). Потенциальный покупатель связывается с администратором «магазина», ему обещают доставить товар после полной оплаты. Оплату предлагают произвести на банковскую карту или на счет через ЕРИП. Однако после получения денежных средств, товар не высылают, а покупателя блокируют.

ФИШИНГ

С целью получения личных данных владельцев счетов мошенники создают страницы-клоны банков, сайтов театров, кальянных и инвестиционных (торговых) бирж.

Для предотвращения подобного необходимо:

- задуматься о причинах низкой цены на товар, отличающейся от цены за тот же товар на сайте или насторожиться почему у магазина нет сайта;
- тщательно проверять информацию о магазине: связаться с продавцом по белорусскому номеру по мобильной связи, а не через Интернет;

- использовать отдельную карту для расчетов в сети Интернет;
- не переходить по ссылкам от неизвестных вам лиц;
- проверять адрес страницы, где вводите данные карты (для белорусских организаций в адресной строке должно быть так: «название сайта».BY/«раздел сайта»);
- подключить в настройках карты бесплатную услугу от банка «3-D Secure».

Стремительное развитие цифровых технологий, резкое увеличение предоставляемых населению числа электронных услуг, а также отсутствие у граждан базовых навыков защиты личной информации в интернете привели к устойчивому росту количества киберпреступлений.

К сожалению, сегодня большинство граждан недостаточно информированы о методике действий кибермошенников, формально относятся к защите собственной информации, персональных данных, а следовательно – имущества.

Виды киберприступлений

1. Финансово-ориентированные киберпреступления

Фишинг

Кибермошенники любят собирать низко висящие фрукты, когда предоставляется возможность заразить компьютеры ничего не подозревающих жертв. В подобных схемах излюбленным средством злоумышленников является электронная почта. Суть метода заключается в принуждении получателя письма к переходу по ссылке от имени легитимной организации

(банка, налоговой службы, популярного интернет магазина и т. д.). В подобных случаях целью, зачастую, является овладение банковскими данными.

Кибервымогательство

Как правило, вначале у пользователя или компании, после загрузки вредоносного кода шифруются файлы, а затем поступает предложение о восстановлении в обмен на денежное вознаграждение (обычно в виде биткоинов или другой криптовалюты).

ФИНАНСОВОЕ МОШЕННИЧЕСТВО

Большинство изощренных схем финансового мошенничества связано со взломом компьютерных систем операторов розничной торговли с целью получения банковских данных о покупателях (так называемые целевые атаки) или последующими манипуляциями полученной информацией.

2. Нарушение авторского права

Это одна из наиболее распространенных форм киберпреступлений. В первую очередь в эту категорию попадает выкладка в общий доступ музыки, фотографий, фильмов, книг и т. д. без согласия авторов.

3. Спам

Спам – чрезвычайно распространенный и многовариантный тип киберпреступлений. Сюда входит массовая рассылка по электронной почте, смс, мессенджерам и другим каналам коммуникации.

Кибербуллинг

Это использование компьютеров и подключенных устройств для домогательств, унижения и запугивания личностей. Граница между кибербуллингом и некоторыми формами преступлений на почве ненависти зачастую размыта.

Способы реализации киберпреступлений

Существует четыре наиболее распространенных способа, которыми пользуются киберпреступники.

1. Использование вредоносных программ. Вероятно, вы понимаете, что существует множество методов эксплуатации систем, и насколько важно использоваться различными мерами безопасности: устанавливать длинные пароли и делать регулярные обновления.

2. DDOS атаки, когда злоумышленник пользуется коммуникационным сетевым протоколом для создания огромного количества запросов к серверу или службе. В этом типе атак главная цель – вывести из строя объект воздействия.

3. Комбинация социальной инженерии и вредоносного кода. Наиболее известная форма подобного рода атак – фишинг, когда жертву принуждают к определенным действиям (нажатию на ссылку в электронном письме, посещению сайта и т. д.), что впоследствии приводит к заражению системы.

4. Незаконная деятельность: домогательства, распространение незаконного контента, груминг и т. д. В этом случае злоумышленники

скрывают свои следы посредством анонимных профайлов, шифрованных сообщений и т.п.

ПРОФИЛАКТИЧЕСКИЕ МАТЕРИАЛЫ

Профилактические листовки здесь https://www.mvd.gov.by/ru/media/photo/326

Профилактическое видео смотрите здесь https://www.mvd.gov.by/ru/media/video

Проверьте свою цифровую грамотность здесь https://madte.st/wwbDI6Hz

Если Вы стали жертвой киберпреступников, обращайтесь в главное управление по противодействию киберпреступности криминальной милиции МВД Беларуси https://www.mvd.gov.by/ru/page/upravlenie-k

Мошенники в киберпространстве и как им противостоять!

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.

Например, злоумышленник связывается с держателем карточки посредством телефонного звонка или со взломанного аккаунта друга, родственника или знакомого в социальных сетях. В ходе звонка или переписки мошенник:

1. Описывает свою сложную жизненную ситуацию и просит помочь ему материально;
2. Представляется работником банка, «запугивает» ложной информацией о сомнительных операциях с банковской платежной карточкой (наличии заявки на кредит, блокировке счета или мошеннических атаках), и предлагает для сохранения оставшихся денежных средств перевести их на новый счет;
3. Представляется потенциальным покупателем товара, объявление о продаже которого было размещено держателем карточки в сети интернет (наиболее популярны платформы по продаже б/у вещей).

Сценарии могут быть разными, а итог один: держатель карточки самостоятельно предоставляет все секретные данные, коды из смс-сообщений банка, логин и пароли.

Помните! Такие случаи не относятся к принципу «нулевой ответственности» держателя карточки, так как конфиденциальные данные злоумышленнику сообщил он сам.

Обращаем Ваше внимание, что телефонный номер мошенника может быть похож на телефонный номер Банка и отличаться одной или несколькими цифрами.

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.

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

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!

МОШЕННИК МОЖЕТ ПРЕДСТАВИТЬСЯ:

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

И НАЗВАТЬ ПРИЧИНУ ЗВОНКА:

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

ОН МОЖЕТ ПОПРОСИТЬ:

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

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.

Управление по раскрытию преступлений в сфере высоких технологий МВД Республики Беларусь