ОТДЕЛЕНИЕ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ

КРИМИНАЛЬНОЙ МИЛИЦИИ

УПРАВЛЕНИЕ ВНУТРЕННИХ ДЕЛ ОРШАНСКОГО РАЙИСПОЛКОМА

ПЛАН-КОНСПЕКТ

по проведению профилактических мероприятий по линии противодействия киберпреступности и Интернет мошенничеств

г. Орша, 2023 г.

На территории Оршанского района количество преступлений в сравнении с аналогичным периодом прошлого года увеличилось почти на четверть.

Ущерб, причиненный жителям области только в первом полугодии текущего года, составил более 100 тысяч рублей. Женщины чаще становятся потерпевшими, чем мужчины, Абсолютное большинство проживает в городах, и имеют высшие образование.

Среди жертв киберпреступников представители практически всех сфер деятельности — бухгалтера, экономисты, директора, заместители директоров частных и государственных учреждений, начальники отделов и управлений учреждений, педагоги, врачи и медицинские сестры, студенты, юристы, программисты и представители других специальностей.

Значительную долю киберпреступлений (более 85%) составляют хищения имущества путем модификации компьютерной информации (ст. 212 УК Республики Беларусь).

Основная часть хищений совершается методами фишинга или вишинга.

ВИШИНГ:

Мошенники чаще всего используют для совершения преступлений звонки в мессенджерах. Звонящие могут представиться сотрудниками банковских организаций или правоохранительных органов. Под различными предлогами они убеждают произвести какие-либо действия, например, передать конфиденциальную информацию, в том числе смс-коды, оформить кредит или установить мобильное приложение.

Вместе с тем, зафиксированы факты, когда мошенники посредством звонков в мессенджерах манипулируют детьми, заставляя их совершать опасные действия.

НАПРИМЕР:

Так, неизвестный мужчина, представившийся сотрудником службы поддержки Viber для обновления мессенджера «посоветовал» 10-летней девочке скачать приложение «RustDesk», а удостоверившись в том, что она дома одна, убедил положить фольгу, а потом куриные яйца в микроволновую печь, каждый раз включая ее на 2 минуты.

В августе 6-летней девочке, мужчина представившейся сотрудником милиции, сказал, что для проверки исправности газовых плит необходимо включить газовую конфорку, выйти из кухни на 30 минут, после чего вернуться и зажечь спичку. Лишь бдительностей соседей, не привела к трагедии.

Что бы избежать подобного рода звонков, в мессенджере «Viber» необходимо активировать функцию «Защита от лишних звонков».

Для включения данной функции необходимо в Viber последовательно нажать следующее: Еще – Настройки – Вызовы и сообщения – Защита от лишних звонков (установить галочку).

Из последних преступлений:

Неизвестное лицо, представившееся сотрудником службы безопасности банка, обманным путем убедило местную жительницу подать заявку на оформление кредита, но потерпевшая, в последний момент была отговорена сотрудницей настоящего банка от совершения подозрительной операции.

Другому местному жителю, под предлогом оказания помощи следствию в поимке преступников, обманным путем убедило подать заявки на получение кредитов в различных банках, на общую сумму более 19000 рублей, после чего с использование программы для удаленного доступа к устройству, совершило хищение данных денежных средств.

ФИШИНГ:

В последнее время вызывает озабоченность рост преступлений совершенных методом фишинга – т.е. способа, цель которого — завладеть реквизитами банковских платежных карт и реквизитами доступа к системе дистанционного банковского обслуживания (СДБО), попросту – Интернет-банкингу. Мошенники умело подделывают различные интернет-ресурсы, которые имеют сервис онлайн-платежей, например, Интернет-банкинг, торговые площадки, службы доставки и другие.

Киберпреступники под любым предлогом вынуждают жертву пройти по ссылке на поддельный интернет-ресурс и ввести на его странице личные данные: реквизиты платежной карты, логин и пароль к сервису, сеансовые ключи от банка или коды подтверждения.

Пользователи, не замечая подмены, на фишинговых сайтах сами вводят свои персональные данные, после чего данные автоматически попадают злоумышленникам. Владея этими данными, мошенники совершают хищения денежных средств со счетов граждан.

Из-за временного отсутствия программ некоторых банков в магазинах приложений для мобильных телефонов, клиентам чаще всего приходится пользоваться – интернет-банкингом, через браузер (Интернет обозреватель). При необходимости найти необходимый банк, поисковая система, может предложить перейти, в том числе, по ссылке в т.ч. на мошеннический (фишинговый) сайт.

Например: sberbank.online или belinvesr24bank.com, вместо sber-bank.by и ibank.belinvestbank.by.

Внешне такой сайт будет идентичен официальному сайту банка.

Мошеннический сайт от официального отличить легко.

Все интернет-ресурсы белорусских организаций расположены в национальном сегменте Интернета – в домене **BY**. Адрес главной страницы сайта должен выглядеть так: **«адрес сайта».BY/**

Например, все тот же: belinvestbank**.by** и другие.

Для других страниц сайта, кроме главной, после последней точки в адресе указывается домен **BY**, а сразу же за ним наклонная черта: **«адрес сайта».BY/**

Например: https://ibank.belinvestbank.by/signin

Из значимых таких преступлений за последнее время: Заместитель директора одной из частных организаций желал оплатить коммунальные услуги через Интернет, нашел в поисковой системе ссылку с логотипом своего банка, и на открытой странице, ввел свои логин и пароль для входа в личный кабинет. Его данные автоматически передались с мошеннического сайта, преступникам и они смогли с его счета потерпевшего, перевести более 13 000 рублей.

Еще один нередкий способ выманивания данных.

На сайтах знакомств мошенники представляются женщинами и заводят виртуальные знакомства с мужчинами. Через непродолжительное время предлагают для личного знакомства вместе сходить в театр, кино или кальянную. Для этого отправляют мужчине ссылку на поддельный сайт театра (кино, кальянной). При покупке билетов мужчина вводит полные данные своей банковской платежной карты, секретный код с ее оборота, предназначенный для совершения расходных операций, а также проверочный смс-код от банка. Так мошенники завладевают его персональными данными и совершают хищение с банковской карты.

Так, мужчина, 24 лет, после знакомства с «Альбиной», для продолжения общения на сайте, одного из «театров», на который он попал, по ссылке от «Альбины», ввел данные своей банковской карты, после чего потерял все свои сбережения.

Примеры сайтов «лжетеатров»: kassa-theatre.com, theater.by-shop.online и другие подобные.

Для белорусских организаций домен должен быть только BY (перед первой наклонной чертой).

<u>Чтобы не стать жертвой киберпреступника:</u>

1. Не выполняйте никаких действий по просьбе незнакомых лиц: не оформляйте кредиты и не устанавливайте непроверенные программы.
2. Пользуйтесь мобильными приложениями (банков, торговых площадок, сервисов услуг).
3. В браузере переходите в интернет-банкинг только с главной страницы банка, для этого нужно кликнуть на разные ссылки (например, курсы валют, кредиты, вклады и т.д.) или по ранее созданной и проверенной Интернет закладки в браузере.
4. Всегда проверяйте адрес и доменное имя сайта, где вводите личные данные. Для белорусских организаций домен должен быть только **BY**. Для разделов сайта, кроме главной страницы, после **BY** должна быть наклонная черта.
5. Активируйте на карте услугу 3-D Secure (подтверждение платежей кодом из смс от банка).

Набирает обороты НОВЫЙ ВИД ВОВЛЕЧЕНИЯ в преступную деятельность.

Гражданам предлагают за вознаграждение оформить на свое имя банковские карты или открыть виртуальные банковские счет, и любым способом передать третьим лицам их реквизиты. Преступники уверяют, что за такие деяния нет никакой ответственности, но это не так. Часто на такие уловки попадаются молодые люди, которые находят подработку в Интернете, и те, кто не имеет постоянного дохода, живет за счет случайных заработков.

Надо знать, что такие действия влекут за собой уголовную ответственность по ст. 222 УК Республики Беларусь за незаконный оборот средств платежа.

Имеются факты, когда в преступную деятельность были вовлечены мать троих детей, молодые девушки, мужчины, не имеющий постоянного дохода и множество случаев, с учащимися колледжей.

Так одна из местных молодых девушек, не догадывалась, что стала звеном в преступной киберцепочки. Всего за неделю через ее карт-счета, переданные ею за вознаграждение, преступники провели несколько десятков тысяч похищенных рублей. Она данную подработку нашла в одной из групп «Telegram» и «сбросила» заказчикам свои паспортные данные и смс-коды с телефона. Благодаря этому мошенники сумели создать виртуальные карты, через которые выводили похищенные у доверчивых граждан деньги.

Нельзя использовать чужую банковскую карту, даже в Интернете.

НАПРИМЕР. *В банкомате мужчина забыл свою банковскую карту. Другой ее обнаружил и сфотографировал с двух сторон, но себе не забрал, а обратно вставил в тот же банкомат. Первый мужчина обнаружил пропажу и вернулся за картой, забрал ее и продолжал пользоваться ей. Так*

как данные его карты уже были скомпрометированы вторым мужчиной, через некоторое время он воспользовался данными и совершил ряд оплат в Интернет-магазине с найденной ранее банковской карты. Действия второго мужчины повлекли за собой уголовную ответственность.

Если бы у первого мужчины в настройках карты была подключена услуга 3-D Secure, он бы был предупрежден через смс-уведомление от банка о попытке операции по его карте в сети Интернет, и смог бы остановить оплату.

Ни в коем случаи нельзя никому давать фотографировать банковскую карту.

Нужно сохранять в тайне свои личные данные для игр.

НАПРИМЕР. *Один из школьников играл в Танки. Другой игрок предложил ему «прокачать» аккаунт, передав на время доступ к аккаунту. После передачи доступа второму игроку в аккаунте был изменен пароль и привязан другой номер телефона, а доверчивый мальчик лишился своего аккаунта и потерял все свои достижения в игре, в т.ч. приобретенные за реальные деньги.*

Через компьютерные игры дети иногда доказывают сою значимость. Но иногда игры переходят в реальную жизнь.

Среди подростков существует мнение, что можно отомстить обидчику, добавив ему проблем. Так иногда подростки на электронную почту организаций и учреждений направляют сообщения о том, что они заминирована. В письме иногда просят перевести деньги, иногда пишут данные отправителя (своего обидчика) письма с расчетом, что за это его привлекут к ответственности.

Надо помнить, что все действия в сети сохраняются и рано или поздно отправитель письма будет установлен. Уголовная ответственность за такие деяния наступает с 14 лет.

НАПРИМЕР. *В Орше отвергнутый молодой человек, желая отомстить новому другу бывшей девушки, отправил от его имени электронное письмо с заведомо ложным сообщением об опасности.*

Ранее другой подросток из области направлял аналогичные письма, чтобы сорвать уроки в школах. В настоящее время в отношении парней возбуждены уголовные дела, им грозит вплоть до 7 лет лишения свободы. Все материальные затраты на работу спецслужб при эвакуации людей придется компенсировать им или их родителям.

Пароли в СОЦ СЕТИ.

Для того чтобы хакеры не завладели деньгами, необходимо соблюдать цифровую гигиену – устанавливать сложные пароли к своим аккаунтам, в Интернете, а также использовать отдельную виртуальную карту, привязывать аккаунт к номеру телефона и подключать двойную аутентификацию.

НАПРИМЕР. *Хакеры взламывают аккаунты в социальных сетях, устанавливают сведения о вас, о ваших родственниках или друзьях, а потом начинают переписываться с вами, просят отправить им что-то личное. Нельзя указывать в Интернете свои реальные данные и данные родственников. Киберпреступники могут шантажировать вас, если у них найдется компрометирующая вас информация, будто личные фото или сообщения.*

Обман с продажей товара

Листая ленту в любой социальной сети, граждане натыкаются порой на крайне заманчивые объявления, где интересующий их товар реализовывается по очень «привлекательной» цене (с большой скидкой). Но в объявлении указано, что срок акции сильно органичен и необходимо спешить, т.к. завтра будет уже поздно. Потенциальные «жертвы» и без какой-либо задней мысли переводят деньги на указанную в переписки с продавцом банковскую карточку. Проходит время, а обещанная им доставка, так и не поступает.

В этой схеме, мошенники создают в социальной сети, страницу магазина. Зачастую это магазин одежды, мебели или электроники, а в период праздников, магазин с соответствующим товаром.

Созданный профиль наполняется фотографиями, украденными из настоящих онлайн-каталогов. Еще для правдоподобности накручиваются подписчики и публикуются «фейковые» отзывы.

Далее всё просто: покупатель оплачивает товар и либо не получает его вовсе, либо ему приходит, совсем не то, что он ожидал. Любые последующие попытки связаться с продавцом чаще всего приводят к попаданию в «черный» список.

Одним и тем же аккаунтом мошенники пользуются несколько раз. И чтобы замести следы своей незаконной деятельности, они меняется название и контент страницы.

Этой преступной схеме можно противостоять. Для этого, перед тем как оформить подозрительно дешевый заказ, нужно не полениться и собрать о данном магазине реальные отзывы и, причем на стороннем ресурсе, а так же проверить реальную стоимость приобретаемых вещей в проверенных интернет-каталогах. Сравним полученную информацию, все встанет на свои места.

Иногда мошенники преднамеренно получают предоплату, позже сообщают, что доставка товара не возможна, и предлагают вернуть деньги обратно, при этом покупателю направляют «фишинговую» ссылку, на которой требуется ввести полные данные карты, включая трехзначный код на обороте, предназначенный только для расходных операций. Под предлогом возврата денег, покупатели иногда становятся дважды обманутыми киберпреступниками.

Отделение по противодействию киберпреступности
криминальной милиции
УВД Оршанского райисполкома

Telegram-канал «Цифровая грамотность»
https://t.me/cifgram