МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ
РЕСПУБЛИКИ БЕЛАРУСЬ

УПРАВЛЕНИЕ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ
криминальной милиции
УВД ВИТЕБСКОГО ОБЛИСПОЛКОМА

ОПОРНЫЙ ПЛАН-КОНСПЕКТ ПО ТЕМЕ:

«ПРОФИЛАКТИКА КИБЕРПРЕСТУПЛЕНИЙ»

Витебск, 2022

Развитие общества не стоит на месте. Компьютерные технологии и Интернет стремительно проникают во все сферы жизнедеятельности человека. Появляются новые виды преступлений. В настоящее время хищение денежных средств с банковских счетов является актуальной проблемой.

Ежедневно около 4-х человек в области становятся потерпевшими от действий киберпреступников. Средний ущерб, причиненный киберпреступлениями, составляет более тысячи рублей. Больше половины потерпевших – женщины. Большинство – со средним специальным и высшим образованием, в возрасте до 40 лет.

Чтобы не стать жертвой киберпреступников, необходимо понимать какие схемы они используют и как уберечь себя от последствий. Вот самые распространенные схемы обмана.

ВИШИНГ Мошенники звонят в мессенджере или по мобильной связи, выдают себя за сотрудника банка. Под предлогом отмены какой-либо операции с деньгами или возврата случайно списанной суммы, выманивают у вас секретные данные: номер, срок действия и трехзначный код на обороте платежной карты. Используя эти сведения, переводят деньги себе на счет.

Или предлагают установить программу якобы для отмены таких операций и назвать код ее регистрации. На самом деле эта программа для удаленного доступа к вашему устройству. Она позволяет злоумышленникам войти в ваш мобильный банкинг и похитить деньги с вашего счета или даже оформить на вас онлайн-кредит.

Иногда к разговору подключаются сообщники, которые представляются сотрудниками милиции или следственных органов, и просят помочь разоблачить мошенника в банке. Для этого необходимо оформить в нескольких банках кредиты и полученные деньги временно перевести на якобы «специальный защищенный счет». При этом мошенники постоянно удерживают свою жертву «на крючке» – не дают закончить разговор, чтобы одуматься, позвонить или поговорить с родными, а также слышать, что происходит вокруг и постоянно держать человека в страхе и напряжении.

Чтобы не стать жертвой киберпреступников, в случае поступления звонка из банка, следует закончить разговор и самостоятельно перезвонить в банк по номеру на обороте платежной карты и уточнить все ли в порядке с вашим счетом.

ФИШИНГ Еще один способ, когда мошенники завладевают персональными данными и совершают хищение денежных средств.

Мошенники точно копируют настоящий и создают фишинговый сайт. Чаще всего подделывают почтовые сервисы (КУФАР, Белпочта, Европочта, СДЭК), но иногда и платежные системы банков

(ОАО «Беларусбанк», ОАО «БелАгроПромБанк»), сервисов оплаты (билетов театра, аренды кальянной). Интернет-адрес в названии похож на настоящий, но имеет отличие в названии или домене. Далее письма, содержащие фишинговую ссылку, рассылаются потенциальным потерпевшим.

Ссылки на поддельные страницы часто присылают в мессенджерах продавцам товаров с сайтов объявлений якобы для получения аванса за продаваемый товар или оформления доставки курьером. Фишинговые страницы содержат сведения о товаре, повторяют фирменный стиль и сервисы сайта, а также используют возможность онлайн-консультанта. Злоумышленник стремится получить все данные карты, в том числе трехзначный код с обратной стороны, а также смс-коды от банка или даже логины и пароли для входа в Интернет-банкинг. Эти данные позволяют ему перевести все деньги с карты владельца, а в случае передачи идентификационного (личного) номера паспорта – оформить онлайн-кредит.

Примеры фишинговых страниц: belpochta.form-by, bellpost.by-card, belpost.be, europocha.be, kufar.cc, bel-bank.online-by и подобные.

Чтобы не стать жертвой киберпреступников, не вводите данные карты на интернет-страницах, открытых по ссылкам из сообщений и даже из поисковых систем. Перед совершением действий со счетом, зайдите на официальный сайт банка, уже с него перейдите в свой личный кабинет или пользуйтесь мобильным приложением банка или торговой площадки.

Помните, что для получения оплаты никогда не требуется вводить трехзначный код с оборотной стороны карты.

В интернет-адресе белорусских организаций после последней точки преимущественно должен быть домен BY, а за ним наклонная черта ***.BY/**

СОЦСЕТИ Злоумышленник, подобрав пароль к аккаунту пользователя соцсети, получает доступ ко всей информации, которая там содержится. Чаще всего он **осуществляет рассылку сообщений интернет-друзьям и ждет отклика, убеждает под разными предлогами перевести денежные средства или передать конфиденциальную информацию, например личные фотографии или данные банковской карты.**

Устанавливайте сложные пароли, используйте цифры и буквы разного регистра.

Активируйте двухфакторную аутентификацию – при входе в ваш аккаунт, будет запрошен код из смс, которая поступит вам на телефон.

Если вам пришло письмо от вашего друга с просьбой одолжить деньги, убедитесь, что это именно он прислал сообщение и нуждается в вашей помощи.

ОБЩИЕ РЕКОМЕНДАЦИИ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ОТ КИБЕРПРЕСТУПНИКОВ

- Никому не доверять по телефону и ни под каким предлогом не передавать номер банковской карты, срок действия, трехзначный секретный код на обороте, логины и пароли доступа к банкингу, смс-коды от банка.
- Подключить услугу «3D Secure» (обязательное подтверждение операций в сети Интернет смс-кодами от банка) и никому не передавать коды (не вводить на страницах).
- При поступлении звонка от работника банка или сотрудника милиции, закончить разговор и самостоятельно перезвонить в банк или милицию.
- Не устанавливать программы по указанию незнакомых лиц.
- Не переводить деньги по указанию, полученному по телефону даже от работников банка или милиции.
- Установить в Вайбер защиту от нежелательных звонков. При поступлении звонка от абонента, не внесенного в телефонную книгу, вы увидите пропущенный звонок и, если нужно, сможете сами перезвонить. (Viber → Еще → Настройки → Вызовы и сообщения → Защита от лишних звонков).
- Настроить ограничения по своей банковской карте: выставить запреты на проведение операций в Интернете, установить максимальные суммы расходов в день (неделю, месяц).
- Не вводить данные своей карты на страницах, открытых по ссылкам.
- В адресе сайта белорусских организаций преимущественно после имени сайта должен быть короткий домен (BY), а после него наклонная черта (***.by/***).
- Тщательно проверять адрес сайта на наличие опечаток — это может быть копия официального ресурса, специально созданного для введения в заблуждение.

Актуальная информация о совершаемых киберпреступлениях доступна в Telegram-канале «Цифровая грамотность»: t.me/cifgram