«ПРОФИЛАКТИКА КИБЕРПРЕСТУПЛЕНИЙ»

Мошенники ищут все новые и новые способы обмана, чтобы завладеть чужими деньгами. Для совершения основных видов киберпреступлений – вишинга и фишинга – они стремятся завладеть номерами белорусских пользователей в мессенджерах, в основном Viber.

Чужие белорусские аккаунты в мессенджере нужны мошенникам, чтобы с бóльшей убедительностью вводить в заблуждение потенциальных жертв, представляясь сотрудниками белорусского банка, правоохранительных органов или просто абонентами оператора связи.

VIBER Для завладения номером мошенники рассылают в чатах и сообществах Viber сообщение со ссылкой, предлагающей получить вам нужную информацию (фейковую новость, предложение о подработке или сведения об успеваемости вашего ребенка). В ссылке обязательно содержатся слова www.viber.com/**activate_secondary**/***. Это и есть маркер мошеннической ссылки. После перехода по такой ссылке пользователь сам дает разрешение на доступ к своей учетной записи в Viber на другом устройстве. Заполучив учетную запись, мошенники имеют возможность читать переписку, скачивать информацию, например, фотографии или данные банковских карточек, или осуществлять рассылку таких же сообщений всем контактам для завладения другими учетными записями.

Если вы предоставили мошенникам доступ к своей учетной записи на другом устройстве, необходимо как можно быстрее его деактивировать. Для этого нужно открыть Viber на своем устройстве, нажать на кнопку в нижнем правом углу «Ещё», зайти в «Настройки», потом в «Учётную запись», «Компьютеры и планшеты» и деактивировать учетную запись на других устройствах.

Чтобы не стать жертвой других киберпреступлений, связанных с хищениями денежных средств, необходимо понимать какие схемы используют злоумышленники и как уберечь себя от последствий.

Вот самые распространенные схемы обмана.

ВИШИНГ.

Мошенники звонят, выдают себя за сотрудника банка. Почти всегда они знают ваше имя. Под предлогом отмены какой-либо операции с деньгами или возврата (сохранения) случайно списанной суммы выманивают у вас данные: номер, срок действия и секретный 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.

Чтобы защитить себя от звонков абонентов не внесенных в вашу телефонную книгу, вы можете настроить «защиту от лишних звонков».

В Viber последовательно нажать «Ещё», «Настройки», «Вызовы и сообщения», поставить галочку напротив «Защита от лишних звонков». В случае поступления звонка с неизвестного номера, он покажется как неотвеченный, при необходимости, вы сами сможете перезвонить.

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

Мошенник точно копирует настоящий и создает 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 есть 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

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).
- Использовать отдельную платежную карту для операций в сети Интернет и хранить на ней сумму, которую вы планируете потратить.
- Настроить ограничения по своей основной банковской карте: выставить запреты на проведение операций в Интернете, установить максимальные суммы расходов в день (неделю, месяц).
- Проверять адрес и домен страницы, на которой вводите данные платежной карты. В адресе сайта белорусских организаций обязательно 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.

Управление по противодействию киберпреступности
криминальной милиции
УВД Витебского облисполкома

страницы содержат сведения о товаре, повторяют фирменный стиль и сервисы сайта, например, онлайн-консультант. 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.by, bellpost.by, belpocht.by, belpost.be, europocha.be, kufar.cc, bel-bank.online.by и подобные.

Чтобы не стать жертвой киберпреступников, перед совершением платежей самостоятельно зайдите на официальный сайт банка, уже с него перейдите в свой личный кабинет.

Переходите в интернет-банкинг только с официального сайта банка, а не по ссылкам, даже из поисковых систем.

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

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

ПАРОЛИ Получив доступ к аккаунту пользователя в соцсети (методом подбора пароля или вредоносного программного обеспечения), **злоумышленник осуществляет рассылку сообщений интернет-друзьям и ждет отклика, убеждает под разными предлогами передать денежные средства или конфиденциальную информацию, например, фотографии или данные банковской карты.**

Устанавливайте сложные пароли, используйте цифры и буквы разного регистра.

Подключите двухфакторную аутентификацию – «привяжите» свой аккаунт к номеру телефона, вы своевременно получите сообщение о попытке входа в ваш аккаунт с другого устройства.

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