ЧТО ТАКОЕ КИБЕРБЕЗОПАСНОСТЬ?

Этим термином называется практика защиты критически важных систем от атак хакеров. Кибербезопасность – это сфера, значение которой сегодня трудно переоценить. Цифровизация неизбежно приводит к необходимости защищать сети и устройства от несанкционированного доступа.

Кибербезопасность представляет собой не только различные программы и запреты, но и принципы работы с людьми. Регулярное обучение сотрудников, информирование о методах злоумышленников не менее важны, чем современный софт.

КАКИЕ ЦЕЛИ ПРЕСЛЕДУЮТ ПРЕСТУПНИКИ?

Получение прибыли – как правило, похищенные данные продаются. Их покупателями нередко становятся либо сами жертвы похищений, надеющиеся вернуть честное имя, либо пользователи «черных» информационных рынков. Чаще всего, после взлома преступники действуют по следующим схемам:

- вывод средств при помощи подделки платежных поручений;продажа данных на просторах даркнета;
- шантаж;
- шифрование и требование выкупа.

КАК НЕ СТАТЬ ЖЕРТВОЙ КИБЕРПРЕСТУПЛЕНИЯ?

1. Никогда, никому и ни при каких обстоятельствах не сообщать реквизиты своих банковских счетов и карт, в том числе лицам, представившимся сотрудниками банка или правоохранительных органов при отсутствиивозможности убедиться, что это те люди, за которых они себя выдают.

В случае поступления звонка от «сотрудника банка» необходимо уточнить его фамилию и номер телефона, после чего завершить разговор и перезвонить в банк самостоятельно. Помните, что реальному сотруднику банка известна о вас следующая информация: фамилия держателя карты, паспортные данные, какие карты оформлены, остаток на счете.

Не следует сообщать в телефонных разговорах, а также при общении в социальных сетях полный номер карты, срок ее действия, код CVC/CVV (находящиеся на обороте карты), логин и пароль к интернет-банкингу, паспортные данные, кодовое слово (цифровой код) из SMS-сообщений.

Если «сотрудник банка» в разговоре сообщает, что с карточкой происходят несанкционированные транзакции, необходимо отвечать, что вы придете в банк лично, ведь все подобные вопросы нужно решать в отделении банка, а не по телефону.

Внимание! *Помните, что сотрудники банковских учреждений никогда не используют для связи с клиентом мессенджеры Viber,Telegram, WhatsApp и пр.*

2. Для осуществления онлайн-платежей необходимо использовать только надежные платежные сервисы, обязательно проверяя доменное имя ресурса в адресной строке браузера. Не следует хранить банковские карты, их фотографии и реквизиты в местах, которые могут быть доступны посторонним лицам. Это же относится к фотографиям и иным видам информации конфиденциального характера.
3. Воздерживайтесь от осуществления онлайн-платежей, связанных с предоплатой и перечислением задатков за товары и услуги, а также благо творительной и спонсорской помощью в пользу организаций и физических лиц при отсутствии достоверных данных о том, что названные субъекты являются теми, за кого себя выдают.
4. Для доступа к системам дистанционного банковского обслуживания (интернет-банкинг, мобильный банкинг), электронным почтовым ящикам, аккаунтам социальных сетей и иным ресурсам необходимо использовать сложные пароли, исключающие возможность их подбора.
5. При поступлении в социальных сетях сообщений от лиц, состоящих в категории «Друзья», с просьбами о предоставлении реквизитов банковских платежных карточек или осуществлении перевода денежных средств в долг, необходимо связаться с данными пользователями напрямую посредством иных средств связи.
6. При обнаружении факта взлома аккаунтов социальных сетей необходимо незамедлительно восстанавливать к ним доступ с помощью службы поддержки либо блокировать, а также предупреждать об этом факте лиц, с которыми вы общались посредством данных социальных сетей.
7. Нельзя открывать файлы, поступающие с незнакомых адресов электронной почты и аккаунтов мессенджеров, а также переходить по ссылкам в сообщениях о призах и выигрышах.
8. Необходимо использовать лицензионное программное обеспечение, регулярно обновлять его и операционную систему, установить антивирусную программу не только на персональный компьютер, но и смартфон, планшет, и регулярно обновлять ее.

Следует ознакомить с перечисленными правилами безопасности своих родственников и знакомых, которые в силу возраста или недостаточного уровня финансовой грамотности могут быть особенно уязвимы для действий киберпреступников.

ПОПУЛЯРНЫЕ СХЕМЫ МОШЕННИКОВ

Схема 1. *Операторы сотовой связи*

Под видом специалистов известных телекоммуникационных компаний мошенники стараются получить доступ к аккаунту человека на «Госуслугах». Они звонят жертве и утверждают, что действующий договор заканчивается и его необходимо продлить, иначе номер передадут другому абоненту. Идти никуда не нужно, все можно сделать по телефону, уверяет злоумышленник. Достаточно продиктовать код из SMS-сообщения.

Лайфхак! *Помните, что вы можете обновить персональные данные, обратившись за услугой лично – в офисе оператора связи или в личном кабинете на его официальном портале (но не по ссылке из SMS). Не называйте никаких данных незнакомым по те-лефону. Если сомневаетесь, позвоните оператору связи по номеру, который размещен на его официальном сайте.*

Схема 2. Предложения от лжеброкеров

Злоумышленники связываются с потенциальными инвесторами через социальные сети или звонят им под видом сотрудников известных инвести-ционных компаний.

Лайфхак! *Помните о простых правилах, которые помогут не по- пасться на удочку инвестиционных мошенников: проверьте сайт инвестиционной компании или брокера, обратите внимание на реквизиты и наличие лицензии Банка России, откажитесь от услуг компании или ее представителей, если они просят перевести деньги за услуги на карту физического лица (либо через электронный кошелек), обязательно заключите договор и запрашивайте отчет об оказании брокерских услуг.*

Схема 3. Общение с работодателем

Собеседование с будущим работодателем – волнительная процедура. Порой мошенники пользуются растерянностью соискателей и крадут личные данные во время онлайн-встречи. Под видом будущего работодателя мошенники проводят собеседование, где они просят кандидата заполнить анкету прямо во время зума. Один из ее пунктов – номер карты и другие ее данные. На нее злоумышленники обещают производить оплату. Некоторые мошенники просят указать информацию по нескольким банковским картам, если какую-то якобы не примет бухгалтерия.

Лайфхак! *Внимательно изучайте предложение от будущего работодателя и отзывы о нем. Не ведитесь на обещания легкого заработка. При общении сохраняйте холодную голову, не поддавайтесь эмоциям, а главное следите за данными, доступ к которым предлагается предоставить.*

Схема 4. Звонки или сообщения от знакомых

Еще одна тактика злоумышленников – рассылка сообщений с просьбой одолжить денег близким или друзьям. Порой в своих сценариях мошенники заходят и дальше – играют на чувствах жертвы и сообщают, что ее родственник попал в беду. Если раньше аферистам приходилось разыгрывать театральный спектакль, подделывая голос, то теперь за них это может сделать искусственный интеллект.

Лайфхак! *Не переходите по неизвестным ссылкам, даже если получили их от близких или знакомых. Договоритесь с родственниками о пароле или секретном вопросе, который нужно назвать, если разговор кажется подозрительным. Такой шаг поможет раскусить намерения мошенников.*

Схема 5. Оплата услуг по фейковому QR-коду

Сегодня, чтобы получить какую-либо услугу или оплатить товар, достаточно навести камеру на QR-код. Например, им можно воспользоваться, чтобы взять в аренду самокат или портативное зарядное устройство для гаджета. Однако вместо прогулки и заряженного аккумулятора телефона можно получить пустой банковский счет.

Лайфхак! *Оплачивайте услугу только через официальное приложение сервиса, а не через камеру гаджета. Или же пользуйтесь только теми QR-кодами, которые размещены на официальных сайтах или в офисах официальных продаж.*

Схема 6. Звонки и сообщения из банка

Наряду с лживыми угрозами об оформлении кредита на имя владельца банковской карты другим человеком или подозрительной операцией по карте появились и новые сценарии. Мошенники под видом специалистов технической поддержки финансовых организаций предлагают установить приложение для поиска вирусов. Еще один популярный сценарий – помощь в сохранении денежныхсредств. Аферисты под видом сотрудников Банка России сообщают жертве о том, что кто-то пытается похитить деньги с ее счета.

Лайфхак! *Пользуйтесь только официальными ресурсами финансовых организаций. Если вам звонят сотрудники банка и разговор с ними кажется подозрительным, перезвоните на официальный номер, размещенный на сайте финансовой организации. Там же вы можете найти ссылки на официальные банковские приложения и скачать их.*

Схема 7. Звонки и сообщения от государственных ведомств

Часто мошенники звонят или пишут человеку от лица сотрудников ФСБ, Росфинмониторинга, ФНС, Социального фонда России, портала «Госуслуги». Самая распространенная уловка – предложение получить какую- либо государственную выплату. Схема классическая: вы нам данные карты, мы вам – деньги.

Лайфхак! *Помните, что подобные ведомства не наделены полномочиями по аресту денежных средств, не оказывают платных услуг по оформлению документов, а также не рассылают подоб- ные письма и не звонят по телефону или в мессенджерах. Если вы получили подобные сообщения – проигнорируйте их и обратитесь напрямую в государственную организацию.*

ЗАКЛЮЧЕНИЕ

Наша жизнь все больше цифровизируется, и представить ее без Интернета уже невозможно. По мере того, как присутствие сети расширяется и углубляется, растет и количество киберугроз. Умение их предотвращать так же важно, как и забота о собственном здоровье и качестве жизни.

Если вы стали жертвой киберпреступников, необходимо сообщить об этом в полицию. Даже если вам кажется, что произошло незначительное мошенничество, ведь вполне вероятно, что вы поможете обезвредить профессиональную группу хакеров. В конце концов, борьба с киберпреступностью – это дело каждого.

Адрес поставщика социальных услуг:

г. Славянск-на-Кубани, ул. Дзержинского, 248

тел.: 8(86146)4-10-05
8(86146)7-36-40
8(86246)2-20-25

Понедельник-четверг с 8.00 до 17.00
Обед с 12.00-12.48
Пятница с 8.00 до 16.00
Обед с 12.00 – 12.40
Суббота, воскресенье – выходной

Государственное бюджетное учреждение социального обслуживания Краснодарского края «Славянский комплексный центр социального обслуживания населения»

отделения развития инновационных форм социального обслуживания

Кибербезопасность: правила, этапы, инструменты

г. Славянск-на-Кубани
2024 г