2. Основные аспекты профилактики киберпреступности

Советы по защите от киберпреступников

Вас беспокоит ситуация с киберпреступностью? Понимание того, что такое киберпреступление, какие типы киберпреступлений существуют и как от них защититься, поможет вам чувствовать себя увереннее.

Что такое киберпреступление

Киберпреступление - это преступная деятельность, целью которой является неправомерное использование компьютера, компьютерной сети или сетевого устройства.

Большинство (но не все) киберпреступления совершаются киберпреступниками или хакерами, которые зарабатывают на этом деньги. Киберпреступная деятельность осуществляется отдельными лицами или организациями.

Некоторые киберпреступники объединяются в организованные группы, используют передовые методы и обладают высокой технической квалификацией. Другие – начинающие хакеры.

Киберпреступники редко взламывают компьютеры по причинам, не имеющим отношения к получению прибыли, например, по политическим или личным.

Типы киберпреступлений

Вот несколько примеров различных типов киберпреступлений:

- Мошенничество с электронной почтой и интернет-мошенничество
- Мошенничество с использованием личных данных (кража и злонамеренное использование личной информации)
- Кража финансовых данных или данных банковских карт
- Кража и продажа корпоративных данных
- Кибершантаж (требование денег для предотвращения кибератаки)
- Атаки программ-вымогателей (тип кибершантажа)
- Криптоджекинг (майнинг криптовалюты с использованием чужих ресурсов без ведома их владельцев)
- Кибершпионаж (несанкционированное получение доступа к данным государственных или коммерческих организаций)

Большинство киберпреступлений относится к одной из двух категорий

- Криминальная деятельность, целью которой являются сами компьютеры
- Криминальная деятельность, в которой компьютеры используются для совершения других преступлений

В первом случае преступники используют вирусы и другие типы вредоносных программ, чтобы заразить компьютеры и таким образом повредить их или остановить их работу. Также с помощью зловредов можно удалять или похищать данные.

Киберпреступления, в результате которых владельцы устройств не могут пользоваться своими компьютерами или сетью, а компании - предоставлять интернет-услуги своим клиентам, называется атакой отказа в обслуживании (DoS).

Киберпреступления второй категории используют компьютеры или сети для распространения вредоносных программ, нелегальной информации или неразрешенных изображений.

Иногда злоумышленники могут совмещать обе категории киберпреступлений. Сначала они заражают компьютеры с вирусами, а затем используют их для распространения вредоносного ПО на другие машины или по всей сети.

Киберпреступники могут также выполнять так называемую атаку с распределенным отказом в обслуживании (DDos). Она похожа на DoS-атаку, но для ее проведения преступники используют множество скомпрометированных компьютеров.

Также, еще есть третья категория киберпреступлений, когда компьютер используется как соучастник незаконного деяния, например, для хранения на нем украденных данных.

Примеры киберпреступлений

Атаки с использованием вредоносного ПО

Атака с использованием вредоносного ПО - это заражение компьютерной системы или сети компьютерным вирусом или другим типом вредоносного ПО.

Компьютер, зараженный вредоносной программой, может использоваться злоумышленниками для достижения разных целей. К ним относятся кража конфиденциальных данных, использование компьютера для совершения других преступных действий или нанесение ущерба данным.

Фишинг

Фишинговая кампания - это массовая рассылка спам-сообщений или других форм коммуникации с целью заставить получателей выполнить действия, которые ставят под угрозу их личную безопасность или безопасность организации, в которой они работают.

Сообщения в фишинговой рассылке могут содержать зараженные вложения или ссылки на вредоносные сайты. Они также могут просить

получателя в ответном письме предоставить конфиденциальную информацию.

Другой тип фишинговой кампании известен как целевой фишинг.

Мошенники пытаются обмануть конкретных людей, ставя под угрозу безопасность организации, в которой они работают.

В отличие от массовых неперсонифицированных фишинговых рассылок сообщения для целевого фишинга создаются так, чтобы у получателя не возникло сомнений, что они отправлены из надежного источника, например, от генерального директора или IT-менеджера.

Распределённые атаки типа «отказ в обслуживании»

Распределенные типа «отказ в обслуживании» (DDoS) - это тип кибератаки, которую злоумышленники используют для взлома системы или сети. Иногда для запуска DDoS-атак используются подключенные устройства IoT (Интернет вещей).

DDoS-атака перегружает систему большим количеством запросов на подключение, которые она рассылает через один из стандартных протоколов связи.

Кибершантажисты могут использовать угрозу DDoS-атаки для получения денег. Кроме того, DDoS запускают в качестве отвлекающего маневра в момент совершения другого типа киберпреступления.

Как не стать жертвой киберпреступления

Итак, теперь, когда вы понимаете, какую угрозу представляет киберпреступность, встает вопрос о том, как наилучшим образом защитить ваш компьютер и личные данные? Следуйте следующим советам:

Регулярно обновляйте ПО и операционную систему

Постоянное обновление программного обеспечения и операционной системы гарантирует, что для защиты вашего компьютера используются новейшие исправления безопасности.

Установите антивирусное ПО и регулярно его обновляйте

Использование антивируса или комплексного решения для обеспечения интернет-безопасности. Антивирусное ПО позволяет проверять, обнаруживать и удалять угрозы до того, как они создадут проблему. Оно помогает защитить ваш компьютер и ваши данные от киберпреступников.

Если вы используете антивирусное программное обеспечение, регулярно обновляйте его, чтобы обеспечить наилучший уровень защиты.

Используйте сложные пароли

Используйте сложные пароли, которые трудно подобрать, и нигде их не записывайте. Можно воспользоваться услугой надежного менеджера

паролей, который облегчит вам задачу, предложив сгенерированный им сильный пароль.

Не открывайте вложения в электронных спам-сообщениях

Классический способ заражения компьютеров с помощью вредоносных атак и других типов киберпреступлений - это вложения в электронных спам-сообщениях. Никогда не открывайте вложение от неизвестного вам отправителя.

Не нажимайте на ссылки в электронных спам-сообщениях и не сайтах, которым не доверяете

Еще один способ, используемый киберпреступниками для заражения компьютеров пользователей, - это вредоносные ссылки в спамовых электронных письмах или других сообщения, а также на незнакомых веб-сайтах. Не проходите по этим ссылкам, чтобы не стать жертвой интернет-мошенников.

Не предоставляйте личную информацию, не убедившись в безопасности канала передачи

Никогда не передавайте личные данные по телефону или по электронной почте, если вы не уверены, что телефонное соединение или электронная почта защищены. Убедитесь, что вы действительно говорите именно с тем человеком, который вам нужен.

Свяжитесь напрямую с компанией, если вы получили подозрительный запрос

Если звонящий просит вас предоставить какие-либо данные, положите трубку. Перезвоните в компанию напрямую по номеру телефона на ее официальном сайте, и убедитесь, что вам звонили не мошенники.

Желательно пользоваться, при этом, другим телефоном, потому что злоумышленники могут оставаться на линии: вы будете думать, что набрали номер заново, а они будут отвечать якобы от имени банка или другой организации, с которой, по вашему мнению, вы разговариваете.

Внимательно проверяйте адреса веб-сайтов, которые вы посещаете

Обращайте внимание на URL-адреса сайтов, на которые вы хотите зайти. Они выглядят легитимно? Не переходить по ссылкам, содержащим незнакомые или на вид спамовые URL-адреса.

Если ваш продукт (банковская платежная карта) для обеспечения безопасности в Интернете включает функцию защиты онлайн-транзакций, убедитесь, что она активирована.

Внимательно просматривайте свои банковские выписки и запрашивайте в банке информацию по любым незнакомым транзакциям. Банк может проверить, являются ли они мошенническими.

Базовые правила «общения» с телефонными мошенниками

Телефонное мошенничество было и остается одним из наиболее распространенных способов обмана граждан. Обычно цель — завладеть чужими денежными средствами. Как понять, что на другом конце трубки мошенники, и как реагировать на подобные звонки:

Основное правило: не сообщайте данные

Это правило даже можно назвать «нулевым» – ни при каких обстоятельствах не сообщайте по телефону свои конфиденциальные данные. Необходимо помнить, что банки и другие легитимные организации никогда не потребуют у вас озвучить код из смс, CVV и так далее. Запрос конфиденциальной информации - самый явный признак мошенничества.

Перезвоните

При малейшем подозрении необходимо завершить звонок и перезвонить на официальный телефон той организации, от которой якобы поступил первичный вызов. В случае банка, например, телефон можно найти на обратной стороне карты, либо в личном кабинете онлайн-банкинга. Стоит отметить, что помимо финансовых организаций и силовых организаций, мошенники также любят представляться сотрудниками вашего сотового оператора.

Задайте контрольный вопрос

Договоритесь с близкими и родственниками о контрольном слове или коротком вопросе, который позволит удостовериться, что звонит не мошенник. Данная мера может показаться чрезмерной, однако часто мошенники пытаются вывести собеседника из равновесия, говоря о том, что близкому человеку грозит опасность. Мы в любом случае должны иметь «холодную» голову и на 100% быть уверенными в том, что звонит именно тот, кого мы слышим, а не робот или злоумышленник.

Никаких ссылок

Не реагируйте на сообщения с незнакомых номеров, в которых указаны ссылки для скачивания стороннего ПО или переход на какие-либо веб-страницы с целью получения, например, выигрыша в лотерее (особенно, если ни в каком конкурсе вы не участвовали) и так далее. Такие действия чреваты установкой на ваш телефон вирусного ПО, а также кражей данных и денежных средств.

Не переводите деньги

Следующий совет вытекает из предыдущего, но стоит его выделить отдельно: игнорируйте сообщения от незнакомых номеров с просьбой перевода денежных средств. Мошенники могут написать от лица близких родственников (причем, не факт, что у вас такие родственники вообще есть – мошенники делают массовые рассылки, стремясь попасть в большее количество людей). Выходом опять же будет звонок с уточнением на номер человека, от лица которого действуют мошенники.

Не перезванивайте

Не стоит перезванивать по незнакомым номерам (если у вас есть такая возможность). Зачастую можно заметить вызов на телефон, который тут же прерывается. Естественное желание - перезвонить, чтобы узнать, кто звонил. Однако мошенники часто используют платные номера – если вы перезвоните на такой номер, с вас начнет списываться поминутная оплата.

Ошибка перевода: свяжитесь с банком

Если вам приходит смс о зачислении средств, а вы не имеете к этому отношения, есть вероятность мошенничества. В случае с балансом мобильного телефона, у человека, который отправил вам денежную сумму, есть возможность оспорить операцию – если вы самостоятельно переведете деньги обратно, мошенники потом еще раз спишут с вас такую же сумму денег. То же самое касается и банковских переводов – лучше не переводить полученные денежные средства самостоятельно, а обратиться в банк с заявлением об ошибочном зачислении.

Проверяйте источники

Так как актуальные новости зачастую становятся еще одним инструментом убеждения у мошенников, всегда стоит перепроверять в официальных источниках информацию, которую сообщает звонящий. Коронавирус для всех является крайне актуальной и острой темой, в связи с чем особо участились случаи мошенничества, связанные с вакцинацией или социальными выплатами.

Все эти правила – базовые при общении с мошенниками, но каждый день изобретаются новые способы обмана. Иногда этому способствует развитие технологической базы, которую злоумышленники также берут на вооружение – к примеру, создание «голосового клона», который способен имитировать речь реально существующего человека, тем самым еще больше втираясь в доверие к потенциальной жертве. Технология пока широко не используется из-за сложностей создания дипфейка, однако стоит подготовиться и к такому. Противостояние подобному типу мошенничества аналогично с мерами защиты от обычного, телефонного – при малейших сомнениях нужно сбрасывать звонок и перезванивать самостоятельно.

Опасность состоит еще и в том, что злоумышленники используют подмену телефонного номера – у абонента высвечивается номер, вроде как похожий на легитимную организацию (например, начинающийся с +357), но на самом деле это звонок с неизвестного мобильного.

Лучше быть наиболее осмотрительным и недоверчивым, чем попасться на удочку мошенников. Украденные суммы ограничиваются лишь только жадностью злоумышленника, поэтому один такой звонок может стать серьезным испытанием. Не забывайте всегда напоминать базовые правила безопасности своим родным и близким, в особенности детям и пожилым людям, так как они наиболее уязвимы.