Как защитить свои сбережения в виртуальном мире

На протяжении текущего года в Республике Беларусь вновь наблюдается рост количества преступлений в сфере информационных технологий. Подавляющее большинство из них составляют хищения денежных средств путем завладения реквизитами банковских платежных карт – ст. 212 (хищение имущества путем модификации компьютерной информации) Уголовного кодекса Республики Беларусь.

Понимание того, что такое киберпреступление, какие типы киберпреступлений существуют и как от них защититься, поможет вам чувствовать себя увереннее.

В этой статье подробно расскажем о том, что такое киберпреступность, от каких угроз и как нужно защищаться, чтобы обеспечить свою безопасности в сети интернет.

Что такое киберпреступление

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

Большинство киберпреступлений 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 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.

Примеры киберпреступлений

Рассмотрим резонансные примеры различных типов кибератак:

1. 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.

Известным мировым примером атаки с использованием вредоносного ПО является атака вымогателя WannaCry, случившаяся в мае 2017 года. Ransomware – это тип вредоносного ПО, который используется для получения денег в обмен на разблокирование устройства/файлов жертвы. WannaCry - это тип программ-вымогателей, которые используют уязвимость компьютеров Windows. Жертвами WannaCry стали 230 000 компьютеров в 150 странах мира. Владельцы заблокированных файлов отправили сообщение с согласием заплатить выкуп в криптовалюте BitCoin за восстановление доступа к своим данным. Финансовые потери в результате деятельности WannaCry оцениваются в 4 миллиарда долларов.

2. 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.

Известный пример фишинг-мошенничества произошел на Чемпионате мира по футболу в 2018 году. По информации Inc, фишинговые электронные письма рассылались футбольным фанатам.

В этих письмах злоумышленники привлекали болельщиков фальшивыми бесплатными поездками в Москву на Чемпионат мира. У людей, которые проходили по ссылке в сообщениях, были украдены личные данные.

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.

3. Распределённые атаки типа «отказ в обслуживании»

Распределенные атаки 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 (Internet of Things – 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.

Известным примером DDoS-атаки является атака на веб-сайт Национальной лотереи Великобритании в 2017 году. Результатом стало отключение веб-сайта и мобильного приложения лотереи, что не позволило гражданам Великобритании играть.

Как не стать жертвой киберпреступления

Теперь, понимая, какую угрозу представляет киберпреступность, встает вопрос о том, как наилучшим образом защитить ваш компьютер и личные данные?

Следующие советы помогут обезопасить себя и сохранить Ваши деньги:

1. **Регулярно обновляйте ПО и операционную систему**

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

2. **Установите антивирусное ПО и регулярно его обновляйте**

Использование антивируса или комплексного решения для обеспечения интернет-безопасности, – это правильный способ защитить вашу систему от атак. 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.

3. **Используйте сложные пароли**

Используйте сложные пароли, которые трудно подобрать, и, по возможности, нигде их не записывайте, особенно в цифровом виде. Можно воспользоваться услугой надежного менеджера паролей, который облегчит вам задачу, предложив сгенерированный им сложный пароль.

4. **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.

5. **Не нажимайте на ссылки в электронных спам-сообщениях и на сайтах, которые Вам не знакомы**

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

6. **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.

7. **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.

8. **Внимательно проверяйте адреса веб-сайтов, которые вы посещаете**

Обращайте внимание на URL-адреса сайтов, на которые вы хотите зайти. Убедитесь, что они выглядят легитимно. Не переходите по ссылкам, содержащим незнакомые или на вид спамовые URL-адреса. Если ваш продукт для обеспечения безопасности в сети интернет включает функцию защиты онлайн-транзакций, убедитесь, что она активирована.

9. Внимательно просматривайте свои банковские выписки

Наши советы должны помочь вам не стать жертвой киберпреступников. Но если все же это случилось, важно понять, когда и как это произошло. Просматривайте внимательно свои банковские выписки и запрашивайте в банке информацию по любым незнакомым транзакциям. Банк может проверить, являются ли они мошенническими.

Теперь вы понимаете, какую угрозу представляют киберпреступники, и знаете, как от нее защититься.