Как обезопасить себя в сфере информационных технологий

Одной из наиболее острых проблем современности выступает кибермошенничество. При этом важно понимать, что никто не застрахован от воздействия злоумышленников. Современная практика показывает, что их воздействию подвержены все слои населения. Их главная цель – установить Ваши уязвимости, а затем заполучить персональные сведения и воспользоваться ими с целью получения собственной выгоды. При этом, Ваши персональные данные могут использоваться злоумышленниками не только для того, чтобы при их помощи получить доступ к банковским счетам и завладеть денежными средствами, но и для того, чтобы совершать преступные действия от Вашего имени в дальнейшем.

Чтобы не попасть на крючок злоумышленников и обезопасить себя важно понимать с чем вы столкнулись.

Кибермошенничество – это противоправные действия, совершаемые с использованием цифровых технологий с целью хищения данных, денег или доступа к конфиденциальной информации.

Современные методы кибермошенничества постоянно эволюционируют, но можно выделить несколько распространённых видов и способов борьбы с ними.

Виды кибермошенничества:

Фишинг (Phishing) – попытка выманить конфиденциальные данные (логины, пароли, данные карт) через поддельные письма, сайты или сообщения. Указанный вид кибермошенничества имеет несколько разновидностей:

1) Смишинг (Smishing) – фишинг через SMS или мессенджеры.
2) Вишинг (Vishing) – телефонные звонки от мошенников, которые представляются сотрудниками банков, госорганов и т.п.
3) Фарминг (Pharming) – перенаправление трафика с легитимного сайта на поддельный через изменение DNS или вредоносное программного обеспечения.
4) Клон-фишинг (Clone Phishing) – копирование реальных писем с заменой вложений или ссылок на вредоносные.
5) Spear-фишинг – целевая атака на конкретного человека или компанию с использованием собранной о жертве информации.
6) Уэйлинг (Whaling) – атака на высокопоставленных лиц (руководителей, финансовых директоров).

Программы-вымогатели (Ransomware) – вредоносные программы, которые шифруют файлы жертвы и требуют выкуп за дешифровку. Такие программы бывают двух типов:

1) Шифровальщики – зашифровывают важные данные (документы, фото, видео).

2) Блокировщики – блокируют основные функции системы (доступ к рабочему столу, мышь и клавиатуру), но не трогают пользовательские файлы.

Кража данных платёжных карт – получение данных карт через взломанные базы компаний, скимминг-устройства или поддельные сайты.

Социальная инженерия – психологические манипуляции для получения доступа к данным. Например, мошенники могут втереться в доверие в соцсетях или мессенджерах, а потом шантажировать жертву, угрожая распространить сведения, которые могут причинить вред Вашей репутации.

Использование искусственного интеллекта – генерация правдоподобных голосовых или видеосообщений от имени знакомых для выманивания денег.

Мошенничество с кредитами – злоумышленники убеждают жертву оформить кредит, утверждая, что это необходимо для «отмены чужого кредита» или «предотвращения мошеннической операции».

Поддельные курьерские доставки – создание фальшивых сайтов курьерских служб для выманивания данных карт при оформлении заказа.

Как бороться с кибермошенничеством:

Для защиты от фишинга следует не переходить по ссылкам из подозрительных писем, SMS или сообщений в мессенджерах, регулярно проверять доменное имя сайтов (ошибки или отличия от оригинала), не вводить личные и финансовые данные на сомнительных ресурсах, использовать программы-антивирусы, которые могут блокировать доступ к фишинговым сайтам, при подозрительном звонке из «банка» или госоргана класть трубку и самостоятельно перезванивать по официальному номеру.

Против программ-вымогателей следует регулярно создавать резервные копии данных на внешних носителях или в облачном хранилище, обновлять операционную систему и программное обеспечение, использовать программы-антивирусы с поведенческим анализом, которые блокируют подозрительную активность, настроить межсетевой экран и ограничить доступ к системе из внешних сетей; внедрить EDR/XDR-системы для мониторинга и быстрого реагирования на инциденты.

Для защиты банковских карт рекомендуется не сообщать CVV/CVC-код, ПИН-код, данные карты и коды из SMS никому, использовать виртуальные карты для онлайн-платежей и не хранить на

них крупные суммы денежных средств, активировать SMS-уведомления о транзакциях и оперативно блокировать карту при подозрительных операциях, не использовать общественный Wi-Fi для банковских операций, не сохранять данные карт в браузере или на устройствах.

Общие меры предосторожности:

1) используйте двухфакторную аутентификацию;

Справочно: двухфакторная аутентификация (2FA – дополнительный уровень защиты, который требует второго подтверждения личности (код из SMS, приложения-аутентификатора, биометрия) при входе в аккаунт. Это усложняет доступ злоумышленников даже при утечке пароля.

2) не храните пароли и данные карт в открытом доступе, не используйте одинаковые пароли для разных сервисов;

3) регулярно обновляйте пароли и используйте сложные комбинации (не менее 12–16 символов);

4) не скачивайте программы из непроверенных источников, не подключать чужие устройства к своему компьютеру;

5) проверяйте политику конфиденциальности сайтов и приложений перед вводом данных;

6) повышайте цифровую грамотность, актуализируйте знания о распространённых схемах мошенничества и способах защиты.

Если вы стали жертвой кибермошенничества, немедленно сообщите об этом в банк, правоохранительные органы и службу поддержки сервиса, где произошла атака.