Как защититься от кибермошенничества.

Правила безопасности в киберпространстве

Благодаря технологическому прогрессу интернет стал неотъемлемой частью нашей повседневной жизни. Он предоставляет нам доступ к информации, позволяет общаться с людьми со всего мира и решать множество рабочих и личных задач. Однако вместе с преимуществами интернет несет в себе массу угроз и рисков, связанных с кибербезопасностью.

В их числе — противоправные действия с целью кражи личных данных, денежных средств, а также незаконного получения доступа к сведениям, составляющим коммерческую или государственную тайну. В связи с тем, что число подобных преступлений и ущерб от них растут с каждым годом, крайне важно знать, как действуют злоумышленники и как им можно противостоять. Мы рассмотрим основные понятия, связанные с киберпреступностью, и правила, которые помогут сохранить важную информацию и личные данные в безопасности.

Основные разновидности киберпреступлений:

- Мошенничество с использованием электронной почты и других интернет-ресурсов.
- Хищение и использование личных данных, например паролей от соцсетей и мессенджеров.
- Кража данных платежных карт и другой финансовой информации.
- Шантаж и вымогательство, в том числе с применением специальных вредоносных программ.
- Получение несанкционированного доступа к государственным или корпоративным данным.
- Онлайн-торговля запрещенными товарами.

Самые распространенные способы кражи денег связаны с созданием фальшивых (фишинговых) сайтов и получением доступа к конфиденциальным данным пользователей. В Беларуси также отмечают рост числа киберпреступлений с применением методов социальной инженерии. Как правило, их жертвами становятся пожилые люди, которые сами сообщают сведения о себе мошенникам, представляющимся сотрудниками государственных органов или банковского сектора. Кроме того, по-прежнему фиксируются случаи крупных утечек персональных данных, которые впоследствии используются злоумышленниками в противоправных целях.

Самые распространенные схемы мошенничества:

- обзвон граждан от имени правоохранительных органов или банков
- создание фальшивых (фишинговых) сайтов для получения доступа к конфиденциальным данным пользователей
- рассылка писем о «крупном выигрыше» по электронной почте
- фальшивые сайты благотворительных организаций/туроператоров/авиакомпаний
- предложение выгодного заработка на подозрительных интернет-ресурсах
- взлом личных аккаунтов пользователей и рассылка сообщений
- лотереи, викторины, победы в конкурсах, где нужно заплатить «налог на выигрыш» или «комиссию за доставку приза»

Правила кибербезопасности и цифровая грамотность

Стоит еще раз обратить внимание, что жертвой кибермошенников может стать каждый, вне зависимости от возраста, образования, социального положения и прочих факторов. Причина в том, что мошенники воздействуют на эмоции человека, а современные технологии позволяют сделать используемые приемы максимально правдоподобными.

Однако противостоять им можно, для этого следует придерживаться ряда простых правил:

- Никому и никогда не сообщайте свои паспортные данные и финансовые сведения: данные карты и ее владельца, трехзначный код с обратной стороны карты или смс-код. Сотрудники банков и госструктур никогда не запрашивают такую информацию.
- Не публикуйте конфиденциальные данные в соцсетях и на каких-либо сайтах.
- Не храните данные карт и pin-коды на компьютере или в смартфоне.
- Если с неизвестного номера звонит сотрудник банка, правоохранительных органов или государственной организации с сомнительным предложением (например, сообщением о попытке оформления кредита или подозрительной операции от вашего имени, обещанием высокого дохода по вкладу, предложением перевести средства на специальный счет и тому подобное) или по телефону запугивают и требуют быстрых действий с финансами, положите трубку.
- Если подозреваете, что вам звонит мошенник, перезвоните в банк или в контакт-центр ведомства, сотрудником которого представлялся звонящий.
- По возможности установите антивирус на все устройства и регулярно его обновляйте.
- Не используйте слишком простые пароли, а также одинаковые пароли для разных учетных записей.
- Защищайте свои аккаунты с помощью двухэтапной аутентификации в тех сервисах, где это возможно. В таком случае мошенники не смогут получить к ним доступ, даже если узнают пароль.
- Совершайте покупки в интернете только на проверенных сайтах. Сравнивайте адреса сайтов, может отличаться одна буква или точка, не попадитесь на сайт-зеркало.
- Никогда не вводите личные и финансовые данные на сомнительных сайтах и не переходите по ссылкам из подозрительных писем, которые предлагают, например, пройти опрос или получить какую-либо выплату.

<u>Если же средства уже переведены мошенникам:</u>

- Немедленно заблокируйте карту с помощью мобильного приложения, личного кабинета на сайте банка или через контакт-центр банка по телефону.
- В течение суток после получения сообщения о списании средств напишите заявление в отделении банка о несогласии с операцией. Также обратитесь с заявлением о хищении денег в любое отделение милиции.

Современный мир и технологии не только дарят нам бесконечный доступ к информации, но и ждут от нас умения ими пользоваться. Развитие критического мышления, соблюдение простых правил информационной гигиены, бдительность и забота об окружающих помогут избежать проблем и не стать жертвой кибермошенников.