**Как защититься от киберпреступников**

Можно ли заблокировать звонки через мессенджеры на телефоны пожилых людей?

Реально ли спасти деньги и куда нужно обращаться при кибератаке?

Что делает уязвимой жертву развода?

Нельзя сказать, что раньше подобных преступлений встречалось намного меньше. Просто их латентность была выше. Криминальная среда переориентировалась на наших граждан. Почему так случилось? Значительно вырос объем банковских услуг, предоставляемых онлайн. Увеличилось количество банковских карт, различных систем дистанционного банкинга, услуг торговых онлайн-площадок, на которых карты используют для расчетов. Это привлекательная среда для злоумышленников, где они увидели большое поле для криминальной деятельности. Осложняется все тем, что большинство граждан не знают, как обезопасить и защитить себя. Немалую роль играют методы социальной инженерии. Еще с 1980-х их применяют хакеры во всем мире, но для наших граждан это в новинку. И когда им звонят и представляются сотрудниками банков, правоохранительных органов, они верят.

Сами методы психологической атаки применяют умело. Человека сразу вводят в шок фразами типа «у вас похищены деньги», «с вашим счетом производятся мошеннические операции». Жертва в стрессе и хочет обезопасить себя. А ей тут же предлагают «решение проблемы», не давая здраво мыслить. Для пострадавшей стороны главное — защитить деньги на счету. А мошенники обещают помочь, но для этого надо предоставить реквизиты банковских карт либо сеансовые пароли — смс-сообщения. В последнее время актуальная схема: потерпевший сам устанавливает на телефон программу для удаленного управления устройством. Затем злоумышленники получают доступ к устройству и всю необходимую информацию, в том числе для интернет-банкинга.

Страдают люди разных возрастных групп, в последнее время больше тех, кто постарше. Мало кто читает договор и использует возможности защиты от банков. Можно подключить, к примеру, смс-оповещение о расходных операциях карты, что обезопасило бы многих клиентов. Если человек увидит в смс, что у него списали деньги со счета, разумеется, отреагирует. В некоторых случаях хищение крупных сумм происходит не одномоментно, а постепенно. Реальный случай: более 200 тысяч долларов снимали со счета владельца карты в течение двух недель. Стояло ограничение по сумме, но человек без смс-оповещения не замечал происходящего. Средства выводят через цепочку банковских счетов.

Это целые сети. Одни ищут тех, кто готов оформить на свое имя подставные банковские счета, сим-карты, и привязывают к системе интернет-банкинга абонентские номера. Их руководитель организует обналичивание. Другие занимаются переводом. Само хищение делится на два этапа: сначала завладевают реквизитами, потом снимают деньги. Есть много способов получить базы данных с вашим телефоном, адресом и т.д. Чаще всего это происходит с помощью взлома интернет-магазинов. Так, к примеру, узнают о том, каким банком пользуется клиент. В некоторых случаях даже неполный номер карты могут использовать, чтобы убедить потерпевшего, будто ему звонит сотрудник безопасности банка.

В интернете могут действовать иностранные граждане, находящиеся за пределами нашей республики. Также иногда используют оборудование, которое размещено в третьей стране. Необходимо направлять запросы за границу для получения нужных сведений. В интернете преступления совершают чаще, потому что это намного легче, чем в случае традиционных краж и хищений. Не стоит никому сообщать конфиденциальные данные, ведь именно на их получение нацелены преступники. В то же время иногда люди быстро реагируют на мошенничество, звонят в банк, и тогда удается вовремя заблокировать карту.

**Чем отличаются фишинг и вишинг?**

При фишинге мошенники используют подставные сайты, направляя по электронной почте или в мессенджерах ссылки на них под различными предлогами, чтобы человек перешел и ввел какую-то информацию. Например, номер карты. А вишинг — это тоже выманивание реквизитов, но через телефонные коммуникации. Явный признак мошенничества — просьба предоставить такую информацию. Если одна схема мошенничества дает сбои, ее корректируют, придумывают новые способы.

Много тревожных моментов, связанных с онлайн-играми. Встречались случаи, когда дети использовали реквизиты родительских банковских карт для покупки игровой валюты или знакомых, друзей. В игровых чатах есть граждане разных государств. Среди них распространен сватинг: чтобы отомстить за неудачу в игре, через специальные сервисы, позволяющие скрыть личность, они направляют сообщения о минировании. Указывают при этом данные своего «обидчика». Это явление вызывает особую озабоченность, ребенок может пострадать невольно. Нужно общаться с сыном, знать, в какие сообщества он входит. Часто эти чаты закрыты. Предупредите ребенка о последствиях: за «шалости» могут привлечь к административной или уголовной ответственности. За преступления против информационной безопасности, к примеру, за продажу чужих аккаунтов в игре, возможно наказание, связанное с лишением свободы.

Важно понимать, что платежный инструмент — не только сама банковская карта, но и ее реквизиты, коды из смс-сообщений, логин и пароль в системе интернет-банкинга. Они могут быть ключом доступа к счету, поэтому передавать их и уж тем более размещать в открытом доступе нельзя. Например, фото карточки в сети. Большинство людей не пострадали только потому, что их никто не пытался взломать. Если такая цель есть, к любому можно найти ключ.

Следите за тем, чтобы информация на карте не попала в чужие руки. Даже без самой карты с нее могут снять деньги. Если вам звонят подозрительные люди, нужно немедленно прекращать разговор и перезванивать по телефонам, указанным либо на карте, либо на сайте банка или в договоре. Поинтересуйтесь, не было ли несанкционированного доступа к счету. Если все же какую-то информацию вы передали, немедленно попросите банковских работников заблокировать карту.

Общая рекомендация: тех, с кем общаешься в интернете, необходимо перепроверять. Даже аккаунт друга может оказаться фейковым. А если что-то продаете через интернет, всегда лучше рассчитаться наличными, без данных карты. Правила информационной безопасности нужно соблюдать, чтобы преступлений было меньше.