Мошенники и современные технологии: как защититься от них?

По материалам информационного агентства «in business kz»

Простые меры предосторожности, которые помогут гражданам уберечь себя и свои деньги от финансовых мошенников.

В последние годы в Казахстане стремительно набирают силу и совершенствуются новые виды мошенничества. Для достижения своего преступного умысла мошенники зачастую используют самые современные технологии.

Напоминаем простые меры предосторожности, которые помогут гражданам уберечь себя и свои деньги от финансовых мошенников. Бесплатный сыр бывает только в мышеловке.

Телефонные звонки

В Сети много историй, как мошенники звонят казахстанцам на мобильный телефон и представляются сотрудниками банков. При этом они грамотно и уверенно изъясняются, используя банковскую терминологию. К примеру, мошенники заявляют, что по платежной карте обнаружены подозрительные операции, и, чтобы их «заблокировать», необходимо вбить в систему данные владельца карты: ИИН, номер телефона, к которому привязана карта, номер банковской карты, номер текущего или сберегательного счета. Когда клиент указывает реквизиты, они просят продиктовать код из SMS-сообщения, отправленного на номер клиента, или набрать его в тоновом режиме на

телефоне якобы для блокирования перевода денег. После получения кода мошенники, как правило, меняют номер телефона в интернет-банкинге клиента и выводят деньги со счетов. Что же делать в такой ситуации? Правильно будет завершить разговор и позвонить в обслуживающий банк, чтобы уточнить информацию. Желательно также написать заявление в банк о попытке совершения мошеннических атак на ваши счета. Есть регламент действий сотрудников банков, в соответствии с которым сотрудники банков никогда не звонят первыми клиенту с требованием предоставить данные по карте либо полученные SMS. Любое общение по данным вопросам инициируется исключительно клиентом.

Ловушки в онлайне

Один из видов финансовых афер связан также с торговыми интернет-площадками, где, как правило, никто не контролирует взаимоотношения продавца и покупателя. Здесь часто работают мошенники «под прикрытием». Они уверяют клиента, что хотят приобрести товар и внести предоплату, но для этого нужны, конечно же, реквизиты платежной карты и код из SMS-сообщения, отправленный на номер клиента якобы для активации перевода денег. Схема аналогична первой, как и результат: лжепокупатели выводят все деньги со счетов и исчезают. Кстати, никогда не отправляйте предоплату, не проверив продавца и товар. Интернет-аферисты могут опустошить ваш счет за считанные секунды, особенно если вы попадетесь «в капкан» фишингового сайта. Это еще одна из разновидностей мошенничества, когда злоумышленники создают клон популярного интернет-магазина, сайта банка либо социальной сети с целью получения реквизитов платежных карт, так называемый фишинговый сайт. И распространяют ссылки на него через имеющуюся базу почтовых адресов, в числе которых может оказаться и ваш адрес. Чтобы знать, как бороться с фишинговыми сайтами, необходимо иметь минимальные знания об Интернете, его использовании и методах защиты информации. Чтобы не попасть на уловки, помните несколько правил: нигде не указывайте свои персональные данные; обращайте внимание на оформление сайта; проверяйте правильность ссылки в адресной строке; пользуйтесь защищенным соединением https; фильтруйте подозрительные письма; не пользуйтесь открытыми точками доступа Wi-Fi для входа в банковские аккаунты. Никому не сообщайте свои конфиденциальные данные: паспортные данные, реквизиты перевода (особенно секретный код перевода).

Простые правила безопасности

Если мошенник владеет достаточной информацией о вас, он может от вашего имени покупать товары и услуги, открывать новые счета, переводить деньги или подавать заявки на получение кредитов. Чтобы такого не случилось, следуйте простым правилам:

- используйте функции безопасности вашего компьютера и мобильных устройств (антивирусная защита, сложные составные пароли с периодической их сменой, не храните на компьютере или мобильном устройстве личные данные в открытом виде);
- избегайте публикаций личных и банковских данных в Интернете (форумы, социальные сети и т. д.);
- не доверяйте звонкам от незнакомцев, которые представляются сотрудниками финансовых организаций, не раскрывайте им свои персональные данные, особенно PIN-код, CVV-код (трехзначный номер на тыльной стороне карты);
- не открывайте электронные письма, полученные из неизвестных или подозрительных адресов, не переходите по ссылкам, присланным из сомнительного источника по электронной почте, в социальных сетях или в SMS;
- если вы часто совершаете онлайн-покупки, то лучше заведите отдельную карту для интернет-покупок; перед совершением онлайн-покупки убедитесь, что сайт, на котором вы находитесь, действительно принадлежит интернет-магазину и его адрес начинается с https://, а не с http://;
- подключите сервис SMS-уведомлений к своим платежным картам; никогда не отключайте функцию 3D-Secure на вашей платежной карте;
- не храните PIN-коды вместе с карточками, и, конечно же, не разглашайте их никому, не передавайте свои банковские карты третьим лицам (даже родственникам), в том числе для проведения платежей в кафе и ресторанах.

Срочно обращайтесь в свой банк, если:

- заметили необычную активность на своих счетах;
- не можете получить удаленный доступ к своим счетам;
- вашу карту не принимают к обслуживанию.

Финансовые пирамиды

Самый известный и распространенный способ отъема денег у граждан на все времена – это финансовая пирамида. Финансовая, или, как по-другому ее называют, инвестиционная, пирамида – это модель получения дохода, где происходит перераспределение денежных средств от вновь привлекаемых участников (нижестоящих) к вышестоящим – так называемой «верхушке» пирамиды.

Самая простая схема финансовой пирамиды: первым участникам организатор платит большой доход из собственных средств, первые участники при этом делают небольшой взнос. Некоторое время организатор пирамиды нарабатывает количество участников и репутацию. Вознаграждение оплачивается из средств новых участников. Когда набирается определенное количество участников и большая сумма, организатор исчезает со всеми деньгами участников. Пирамиды с такой схемой часто позиционируют себя как инвестиционные или благотворительные фонды. Каковы признаки финансовой пирамиды?

Рассмотрим основные из них:

1. Вас просят сделать вступительный взнос, просят привести новых клиентов и т. п.
2. Обещание высокого вознаграждения, выплаты денежных средств новым участникам из вносов других вкладчиков.
3. Отсутствие лицензии финансового регулятора на осуществление деятельности по привлечению денежных средств.
4. Агрессивная реклама, в которой организация публично обещает неслыханно высокий доход, в несколько раз превышающей рыночный уровень.
5. Нет точного определения деятельности организации или маскировка под некоторые виды деятельности (инвестиционная компания, сетевой маркетинг, потребительский кооператив др.).

Если организация, которой вы хотите доверить свои деньги, обладает хотя бы несколькими из перечисленных признаков, стоит задуматься, не пытаются ли вас вовлечь в финансовую пирамиду? Как видите, ловушек много как в онлайне, так и в офлайне. Попадают в них люди разных возрастов и материального положения. Конечно, отчаявшийся заемщик, у которого возникли трудности с оплатой кредита, охотнее поверит мошенникам, которые работают якобы в легальной посреднической фирме и предлагают «договориться» с банком, чтобы списать кредит за небольшую плату. Некоторые казахстанцы верят мошенникам, обещающим избавить их от «кредитного рабства» или за символическую сумму «переписать» кредитную историю, передают им, помимо денег, данные своих документов, удостоверяющих личность, ЭЦП и иные ценные сведения. Этой информации мошенникам достаточно, чтобы обналичить деньги с карты или «повесить» на вас чужой кредит.