Координационный центр по вопросам формирования у молодежи активной гражданской позиции, предупреждения межнациональных конфликтов, противодействия идеологии терроризма и профилактики экстремизма УрФУ

Уральский федеральный университет имени первого Президента России Б.Н.Ельцина

ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО

Две трети россиян за последний год сталкивались с телефонным мошенничеством. 67% опрошенных россиян сообщили о том, что им звонили телефонные мошенники за последний год.

Мошенники в 2023 году похитили в РФ у клиентов банков 15,8 млрд руб., что на 11,5% больше, чем годом ранее.

Кем чаще всего представляются телефонные мошенники:

- родственники, знакомые *(к вам могут обратиться не только по телефону, но и написать в социальных сетях с аккаунта близкого человека. Помните, что его могли взломать и, если вас просят срочно перевести деньги, то лучше связаться с этим человеком другим способом.)*
- сотрудники банка *(фейковые менеджеры банка или сотрудники службы безопасности банка могут обращаться к вам под разными предлогами и требовать предоставить личные данные или данные вашего лицевого счёта, чтобы получить к нему доступ)*
- представители сотового оператора *(также могут к вам обратиться под видом менеджера и под разными предлогами просить вас сообщить код из СМС или другие данные, которые позволят получить доступ к вашей учетной записи на Госуслугах, банковскому счёту и другим важным данным)*
- сотрудники силовых структур и государственных служб *(такие мошенники, как правило, обладают вашими личными данными, включая прописку, данные паспорта, родственные связи, и готовы инсценировать целую «спецоперацию» по хищению ваших денежных средств и действовать обманом, угрозами и другими методами)*

Мотивацией мошенников могут быть не только корыстные, но и политические мотивы. Участились случаи мошенничества и хищения средств с целью вербовки и принуждения к противоправной деятельности.

Признаки мошенничества:

- На вас выходят сами *(любой неожиданный звонок или СМС с незнакомого номера – это повод насторожиться)*
- Вас радуют внезапной выгодой или пугают неприятными последствиями *(сильные эмоции могут притупить вашу бдительность)*
- Говорят о деньгах *(вам предлагают спасти сбережения, получить компенсацию или удачно вложить деньги)*
- Просят сообщить персональные данные *(Злоумышленников интересуют реквизиты ваших счетов, пароли и коды из СМС и банковских уведомлений)*
- С вами связываются с помощью мессенджеров *(Звонок поступает через мессенджеры WhatsApp или Telegram, где его сложнее отследить)*

Типичные сценарии мошенничества:

1. Мошенничество с банковскими картами

На телефон приходит сообщение о блокировке банковской карты и предлагается бесплатно позвонить на определенный номер для получения подробной информации. Когда абонент звонит по указанному телефону, мошенник сообщает, что на сервере, отвечающем за обслуживание карты, произошел сбой, а затем просит сообщить номер карты и ПИН-код для ее перерегистрации.

Возможен вариант, когда преступник, представившись работником банка, сам звонит абоненту с целью получения ПИН-кода банковской карты.

2. Спасение денежных средств\защита от мошенников

Вам звонят из вашего банка и просят подтвердить, что вы оформили кредит на большую сумму денег, когда вы опровергаете эту информацию вам сообщают, что мошенники пытаются оформить на вас кредит. Далее Вам предлагают проделать ряд действий, чтобы защитить свои денежные средства, например: скачать стороннее приложение, сообщить коды из смс, перевести деньги на некий «безопасный счёт в другом банке», и как только жертва переводит средства, мошенники исчезают, а пострадавший получает оформленный на него кредит.

3. Акция оператора мобильной связи/истечение срока договора по оказанию услуг связи

Абонент получает сообщение/звонок об акции, проводимой его мобильным оператором. Например, предложение подключить новую эксклюзивную услугу, получить на какой-то период времени возможность осуществлять бесплатные звонки по стране и другие. Однако, для этого ему необходимо отослать в службу информационной поддержки по сообщенным телефонам коды нескольких карт оплаты\код из СМС. Естественно, потом выясняется, что оператор рекламных акций не проводил, а карты оплаты и коды из СМС пополнили счета мошенников.

4. Просьба о помощи

Поступает звонок с незнакомого номера, и мошенник, представившись родственником, знакомым или коллегой по работе, взволнованным голосом сообщает, что задержан сотрудниками полиции и обвинён в совершении какого-нибудь преступления. Далее в разговор вступает второй мошенник и представляется сотрудником правоохранительных органов. Он уверенным голосом сообщает, что совершено преступление и, если Вы хотите помочь, необходимо привезти определенную сумму в оговоренное место и передать какому-либо человеку или перевести на указанный счёт.

5. Звонок на платный телефонный номер

Абоненту приходит SMS с просьбой перезвонить на указанный номер мобильного телефона. Просьба может быть обоснована любой причиной – помощь другу, изменение тарифов связи, проблемы со связью или с банковской картой и так далее. После того как абонент перезванивает, его долго держат на линии, и, когда он отключается, то оказывается, что с его счёта списаны крупные суммы.

6. Выигрыш приза

На мобильный телефон приходит смс-сообщение о выигранном призе либо поступает звонок с поздравлением в выигрыше в лотерее, акции и т.п. и необходимости связаться с «призовым» отделом. После того, как владелец телефона связывается с автором сообщения («призовым» отделом), его убеждают в честности акции и сообщают, что необходимо предварительно оплатить сопутствующую услугу или подоходный налог через систему денежных переводов. В итоге жертва лишается переведённой суммы денег, а «призовой» отдел перестаёт выходить на связь.

Координационный центр по вопросам формирования у молодежи активной гражданской позиции, предупреждения межнациональных конфликтов, противодействия идеологии терроризма и профилактики экстремизма УрФУ

Уральский федеральный университет имени первого Президента России Б.Н.Ельцина

Как обезопасить себя от телефонного мошенничества?

1. не отвечайте на звонки с незнакомых номеров;
2. не говорите никому коды из СМС;
3. не берите кредиты, чтобы спасти деньги;
4. не переводите деньги на чужие счета;
5. не переходите по ссылкам даже от знакомых номеров;
6. не сообщайте данные вашей банковской карты;
7. не скачивайте программное обеспечение/приложения с неофициальных сайтов.

Единый номер вызова экстренных оперативных служб Тел.: 112

Дежурный отдела ФСБ. Тел.: +7 (343) 358-63-41

Дежурный по МВД. Тел.: +7 (343) 358-70-71 или 02