«Ваш аккаунт под угрозой»: как мошенники играют на эмоциях пользователей

Еще несколько лет назад интернет-мошенничество ассоциировалось в основном со странными письмами о наследстве от неизвестных родственников. Сегодня схемы стали куда тоньше. Мошенники научились копировать интерфейсы банков, подделывать сайты известных сервисов и, главное, - очень точно давить на человеческие эмоции.

Эмоции в онлайне

В одних случаях мошенники пугают людей потерей данных и блокировкой аккаунта. В других - обещают легкие деньги или дорогие призы. А иногда используют самое сильное оружие - доверие к друзьям и близким.

Первая схема, о которой предупредила Генеральная прокуратура Казахстана, построена на страхе потерять аккаунт, данные или даже весь смартфон. Злоумышленники массово рассылают владельцам iPhone сообщения о том, что их iCloud якобы переполнен. Пользователя торопят: если срочно не обновить данные, фотографии и документы будут удалены, а аккаунт - заблокирован. В некоторых случаях потенциальным пострадавшим напоминают, что без аккаунта потеряет смысл и само устройство, ведь аккаунт якобы «вшит» в него.

Жертва переходит по ссылке, попадает на поддельный сайт Apple ID или электронной почты и сам передает мошенникам логин, пароль, а иногда и банковские данные. Аналогичные атаки уже распространяются от имени Google Drive, Mail.ru и Яндекс Диска.

Особенность современных схем в том, что они почти никогда не строятся только на технологиях. В случае с iCloud мошенники играют на страхе потерять личные данные. У многих в облаке хранится буквально вся цифровая жизнь: фотографии детей, рабочие документы, переписки, контакты.

Но страх — далеко не единственный инструмент.

«Поздравляем! Вы выиграли iPhone»

Если схема с iCloud давит на тревогу, то здесь работает другая эмоция - жадность и азарт. Человеку приходит сообщение в WhatsApp, Telegram, SMS или на почту: «Поздравляем! Вы стали победителем розыгрыша iPhone / 1 000 000 тенге / автомобиля».

Иногда мошенники прикрываются именами известных брендов, банков или маркетплейсов. Особенно часто - крупными экосистемами, которым люди привыкли доверять. Например, в Казахстане уже фиксировались фальшивые «розыгрыши» от имени пяти ведущих банков страны и других популярных сервисов, например, доставки и покупки товаров.

Дальше сценарий развивается одинаково:

- пользователя просят перейти по ссылке;
- ввести ИИН или данные карты;
- оплатить «комиссию за получение приза»;
- подтвердить личность SMS-кодом.

В этот момент деньги и данные оказываются у мошенников.

Суммы обычно небольшие — 500, 1000 или 2000 тенге. Именно поэтому многие не воспринимают операцию как рискованную. Но после ввода данных мошенники получают доступ к карте или начинают списывать деньги повторно.

Иногда схема усложняется. Пользователю показывают поддельный сайт с «таблицей победителей», комментариями «счастливчиков» и счетчиком оставшихся призов. Все это создает иллюзию реальности происходящего.

Парадокс таких схем в том, что человек часто понимает нелогичность происходящего - но желание получить «подарок» отключает критическое мышление. Именно поэтому мошеннические розыгрыши остаются одной из самых живучих схем интернета.

«Проголосуйте за племянницу»

Еще одна схема, которая массово распространяется через WhatsApp и Telegram, выглядит максимально безобидно.

Сообщение приходит якобы от знакомого человека: «Привет! Проголосуй, пожалуйста, за племянницу. Она участвует в конкурсе, осталось совсем немного до победы».

К сообщению прикреплена ссылка на «голосование». Сайт выглядит правдоподобно: фотографии детей, счетчики голосов, логотипы конкурса. Но чтобы проголосовать, пользователю предлагают ввести номер телефона и код из SMS.

На деле это код доступа к аккаунту WhatsApp или Telegram. После его передачи мошенники получают полный контроль над мессенджером жертвы.

Дальше схема начинает распространяться как вирус:

- от имени владельца аккаунта друзьям рассылаются новые ссылки;
- знакомых просят срочно занять деньги;
- мошенники получают доступ к перепискам и контактам.

В Казахстане подобные случаи уже неоднократно обсуждались в соцсетях: люди рассказывали, как после одного «голосования» теряли доступ к мессенджеру буквально за несколько минут.

Получив достаточно много информации, мошенники могут делать уже не массовые, а точечные рассылки с индивидуальным подходом и длительной «обработкой жертвы».

Например, взломав аккаунт одного известного коллекционера, мошенники писали его знакомым с просьбой одолжить некоторую сумму на покупку особенно интересных экспонатов. Те, кто был «в теме», думали, что действительно помогают заполучить редкость и несколько человек направили деньги. Не смутила их даже нестандартная банковская карта, на которую просили сделать перевод.

Именно поэтому такие атаки особенно опасны: человек доверяет сообщению, потому что оно приходит не от незнакомца, а от реального контакта.

«Вам пришла посылка»

Еще одна популярная схема последних месяцев связана с доставкой. Приходит сообщение: «Ваша посылка задержана», «Подтвердите адрес доставки», «Оплатите таможенный сбор». Особенно часто мошенники используют названия популярных маркетплейсов и курьерских служб. На фоне роста онлайн-покупок такие сообщения выглядят правдоподобно - многие действительно ждут доставку.

После перехода по ссылке пользователя просят:

- авторизоваться;
- указать банковские данные;
- оплатить небольшую «комиссию».

В некоторых случаях ссылка ведет на страницу установки вредоносного приложения, которое получает доступ к SMS и банковским уведомлениям.

«Это фото с вами?»

Старая схема, которая снова набирает популярность в мессенджерах. Пользователю приходит сообщение: «Это ты на фото?» или «Посмотри, что про тебя написали». Внутри - ссылка или файл. После открытия устройство может заразиться вредоносным ПО, мошенники получают доступ к аккаунтам или начинается автоматическая рассылка по контактам. Иногда ссылка ведет на фишинговую страницу входа в Telegram или Instagram.

Главная задача - вызвать сильную эмоциональную реакцию: любопытство, тревогу или страх.

Почему люди продолжают попадаться

Многие уверены: «Со мной такое не случится». Но современные мошеннические схемы как раз и рассчитаны на обычных людей, а не на технически неподготовленных пользователей.

Именно поэтому специалисты по кибербезопасности постоянно повторяют: главная защита сегодня - не антивирус, и не система безопасности банка или приложения, а привычка остановиться и перепроверить информацию.

Как защитить себя от подобных схем:

1) Не переходите по ссылкам из сообщений. Даже если письмо или SMS выглядят официально.

2) Проверяйте информацию только через официальные приложения и сайты. Хотите проверить iCloud или банковский аккаунт - зайдите туда самостоятельно.

3) Никому не сообщайте коды из SMS. Даже друзьям и родственникам.

4) Не верьте в «слишком хорошие» выигрыши. Если вы не участвовали в розыгрыше - вы ничего не выигрывали.

5) Всегда перепроверяйте просьбы знакомых. Лучше позвонить человеку напрямую.

6) Включите двухфакторную аутентификацию. Это значительно снижает риск взлома аккаунтов.

Если аккаунт уже украли - действуйте сразу. Смените пароль, завершите активные сессии и предупредите контакты о взломе.

Сегодня мошенники взламывают не столько устройства, сколько эмоции людей. И чем убедительнее становятся цифровые схемы, тем важнее сохранять привычку не реагировать на сообщения автоматически - даже если они выглядят срочными, выгодными или очень «человеческими».

Материал подготовлен при помощи www.fingramota.kz