КАК НЕ СТАТЬ ЖЕРТВОЙ МОШЕННИКОВ: НЕСКОЛЬКО ОЧЕВИДНЫХ, НО ВАЖНЫХ СОВЕТОВ

Никому не говорите коды из SMS
Это правило № 1 в борьбе с мошенниками. Конечно же, вы о нём слышали. Но мы всё-таки напомним ещё раз, что сотрудники банков такую информацию никогда не спрашивают, а вот мошенники будут ей крайне рады. Получив код, они могут войти в ваш онлайн-банк, чтобы вывести деньги, либо с вашей карты оплатить покупку на каком-нибудь сайте.

Если позвонивший вам человек представляется сотрудником МТС и под каким-нибудь предлогом просит передать ему код из SMS или вашу персональную информацию — сразу прекращайте разговор. Позвонить от МТС может, но никаких паролей и личных данных он требовать не станет.

Берегите данные банковской карты

Постарайтесь не «светить» данные своей банковской карты, особенно если речь идёт об оплате на незнакомом ресурсе. Но главное — никогда никому не сообщайте CVC-код. Это три цифры на оборотной стороне вашей банковской карты, которые служат PIN-кодом для онлайн-транзакций. Если кто-нибудь спрашивает у вас такой код, это повод насторожиться. Для обычных переводов на карту такая информация не требуется, но вот, завладев ею, мошенники легко могут похитить ваши деньги.

«Безопасных» счетов не существует

Довольно часто мошенники играют на страхе людей потерять свои деньги. Если человек начинает паниковать и действовать на эмоциях, злоумышленникам не составит труда обвести его вокруг пальца.

Вот одна из популярных схем развода: вам звонит «сотрудник» службы безопасности вашего банка, ЦБ РФ или даже правоохранительных органов. Он сообщает, что кто-то пытается похитить деньги с ваших счетов, и предлагает план спасения: вывести средства на «безопасный» счёт. Так вот: никаких «безопасных» счетов не существует, это очередная уловка злоумышленников и способ выманить у вас деньги. Если всё же беспокоитесь, всё ли в порядке с вашими счетами, рекомендуем самостоятельно обратиться в службу поддержки банка или проверить состояние счетов в банковском приложении.

Не доверяйте собеседникам-незнакомцам, относитесь критически ко всей информации с их стороны и проверяйте её самостоятельно. Если речь идёт об операциях со счетами — свяжитесь с банком сами. Кто-то сообщает, что ваш родственник попал в беду и ему нужны деньги — позвоните близкому и уточните, всё ли у него в порядке. Скорее всего, он ни о каких своих проблемах даже не подозревает.

Не верьте обещаниям лёгких денег

В письме сообщают, что вы выиграли много денег в лотерею, в которой вы даже не участвовали? Однофамилец из Уганды хочет подарить вам дом и нужно отправить несколько долларов его адвокату, чтобы оформить сделку? Или вам завещал крупную сумму троюродный дедушка, о котором вы даже не слышали, и требуется оплатить пошлину для вступления в наследство? Рекомендуем сразу такие письма удалить, а отправителей заблокировать.

А ещё только мошенники обещают «заработок в интернете без вложений», инвестиции под 500% годовых и прочие золотые горы за пару кликов мышкой. Такие громкие слова обычно означают лишь одно: что вас пытаются обмануть. Исход таких историй обычно один: после того, как жертва перечисляет деньги, все эти инвесторы и адвокаты из Уганды сразу же пропадают.

Запомните: перечислять деньги незнакомцам в интернете — почти всегда плохая идея. И даже если в личку написал любимый блогер с предложением увеличить ваш заработок, относитесь к таким сообщениям критически и не спешите соглашаться — ведь мошенники часто выдают себя за известных

персон.

Не торопитесь переходить по ссылкам из сообщений

Это касается не только посланий от незнакомцев: даже со знакомыми будьте внимательны. Аккаунт любого из них могут взломать, чтобы отправить всем контактам вредоносные ссылки, несущие в себе вирус или открывающие доступ к вашим личным данным. Киберпреступники активно этим пользуются.

И ещё внимательно смотрите на адрес ссылки: как правило, мошенники просто переставляют буквы или добавляют лишние символы, чтобы казалось, что ссылка ведёт на знакомый вам адрес. Например, avitto.ru или sales_avia. Заметили что-то странное или увидели, что email отправителя похож на сборную солянку из знаков и букв? Не отвечайте на письмо и не кликайте по ссылкам. Сразу отправляйте в спам.

Слишком низкие цены — это всегда подозрительно

Большая распродажа, выгодная акция, огромные скидки и низкие цены — все эти предложения сбивают с толку и заставляют терять бдительность. Прежде чем срочно оплачивать заказ в интернет-магазине, почитайте, что пишут об этом сайте (и пишут ли вообще) другие пользователи.

Критически оценивайте всю информацию, которую сможете найти. Если подавляющее большинство откликов только положительные, но при этом они написаны как под копирку и сводятся к тексту «как здорово, что я совершил покупку», это повод насторожиться. Даже про работу крупных онлайн-площадок обязательно есть негативные отзывы.

Не стоит экономить, если вы не уверены в качестве товара или надёжности магазина. Ни в коем случае не покупайте технику в неизвестных онлайн-магазинах, если её нельзя проверить перед оплатой или на неё не распространяется гарантия.

Материал по теме
Как вычислить телефонного мошенника: пять явных признаков

Настройте двухфакторную идентификацию в приложениях

Двухфакторная аутентификация — это дополнительная защита. Она нужна, чтобы никто не смог воспользоваться вашими аккаунтами, кроме вас. Если двухфакторная аутентификация настроена, для входа в приложение или сервис будет недостаточно просто ввести пароль — также понадобится, например, получить код по SMS на номер, к которому привязан аккаунт. Такую защиту стоит включить везде, где она доступна.