

Чек-лист

Телефонное мошенничество. Правила безопасности.

Телефонное мошенничество известно давно – оно возникло вскоре после массового распространения домашних телефонов.

В настоящее время, когда широко используются мобильные телефоны и личный номер может быть у всех, от десятилетнего ребёнка до восьмидесятилетнего пенсионера, случаи телефонного мошенничества растут с каждым годом.

Напоминаем, что чаще всего в сети телефонных мошенников попадают пожилые или доверчивые люди. При этом каждый человек может стать жертвой мошенничества, если не будет следовать простым правилам безопасности.

Как защитить персональную информацию? Изучите перечень действий, которые помогут обезопасить вас от мошенников и их махинаций:

1. Установить ПИН-код на SIM-карту, чтобы при утере или краже телефона было сложнее воспользоваться вашим номером.
2. Запретить возможные действия с доверенностью. Это делается в ближайшем офисе мобильного оператора. Мошенники не смогут сделать дубликат симки по поддельной доверенности.
3. Установить на смартфон антивирус. Специальная программа защитит устройство от троянов и прочего вредоносного ПО.
4. Обновлять ПО на телефоне по мере необходимости. Обновления безопасности помогут защититься от атак и закрыть уязвимые зоны.
5. Настроить подтверждение банковских операций через push-уведомления. Этот вариант более надежен, чем протокол SMS, который подвержен регулярным атакам.
6. Отказаться от услуги «Мобильный перевод», чтобы мошенники при компрометации SIM-карты не вывели с нее средства.
7. Настроить смартфон так, чтобы он не выводил тексты и уведомления на заблокированный экран.
8. Подключить оповещения об операциях по банковской карте для быстрого определения мошеннических списаний.
9. Оплачивая покупки в интернете, вводить данные карты во всплывающем окне. Мошенники виртуозно копируют страницы оплаты, а копии ведут уже на их сервера.
10. Убрать из папки «Спам» телефонные номера мобильного оператора и банков, в которых вы обсуживаетесь, чтобы вам вовремя приходили оповещения о безопасности.
11. Выбрать банк, через кол-центр которого невозможно изменить привязанный телефонный номер. Это один из способов, которыми мошенники получают персональные данные.
12. Воспользоваться опцией или приложением, блокирующим нежелательные звонки.

