КАК НЕ СТАТЬ ЖЕРТВОЙ КИБЕРМОШЕННИКОВ?

- Не отвечайте на звонки с незнакомых номеров
- Прервите разговор, если он касается финансовых вопросов
- Не торопитесь принимать решение
- Проверьте информацию в Интернете или обратитесь за помощью к близким родственникам
- Самостоятельно позвоните близкому человеку / в банк / в организацию
- Не перезванивайте по незнакомым номерам

ЧТО ВЫДАЕТ ЗВОНОК МОШЕННИКОВ?

- Вам звонят через мессенджер
- Вас торопят
- Давят авторитетом
- Вам отказывают во втором мнении
- Спрашивают код из СМС
- Обещают выгоду без усилий
- Звонят в неудобное время
- Спрашивают код с обратной стороны карты
- Просят установить приложение на смартфон

ЧТО ДЕЛАТЬ, ЕСЛИ МОШЕННИКИ ПОХИТИЛИ ДЕНЬГИ С КАРТЫ?

- **Сразу же заблокировать карту** в мобильном приложении банка звонком на горячую линию банка личным обращением в отделение банка
- **В течение суток сообщите в банк**
- **Как можно скорее напишите заявление в полицию** при личном обращении в ближайший отдел ОВД

ПРОТИВОДЕЙСТВИЕ КИБЕРМОШЕННИКАМ: МЕРЫ БАНКА РОССИИ

- Обмен информацией с МВД России
- Самоограничение онлайн-операций
- Отключение каналов ДБО дропам
- Новый порядок возврата похищенных денежных средств
- Внедрение периода охлаждения

Буклет разработан Региональным центром финансовой грамотности Республики Адыгея при финансовой поддержки Министерства образования и науки Республики Адыгея

КИБЕРМОШЕННИЧЕСТВО

Кибермошенничество появилось и развивается в Интернет-пространстве. Один из самых быстроразвивающихся преступных «бизнесов». Злоумышленники ни на шаг не отстают от технического прогресса. Они постоянно модифицируют свои преступные схемы, повышают их конверсию, подстраивают свои легенды под актуальные информационные поводы.

Кибермошенничество - один из видов киберпреступлений, целью которого является причинение материального или иного ущерба путем хищения личной информации пользователя (номера банковских счетов, паспортные данные, коды, пароли и др.)

ВИДЫ КИБЕРМОШЕННИЧЕСТВА

Фишинг (от англ. слова «fishing» – рыбалка) - вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей (логинам и паролям). Предполагает рассылку писем, замаскированных под послания от легитимных отправителей, а также заманивание пользователей на поддельные ресурсы. Злоумышленники выдают себя за известные интернет-магазины, компании, сервисы. **Цель** – добиться, чтобы пользователи переходили по ссылкам из сообщений, оставляли личную и платежную информацию на фейковых ресурсах.

Вишинг – это разновидность кибер-преступлений, направленных на кражу личной информации по телефону. **Цель** вишинга — узнать данные жертвы: номер карты, код из смс, данные паспорта, пароль от соцсети.

Смишинг — это смесь английских слов sms и phishing, то есть «фишинг по смс». У мошенников могут быть ваши личные данные. Не стоит доверять сообщению только потому, что к вам обратились по имени и указали номер банковской карты.

Излюбленный прием мошенников — срочность. Если от вас требуют срочно спасти деньги, перезвонить в ФСБ или получить выигрыш в лотерею, иначе все пропало,— скорее всего, вам написали мошенники. Возьмите паузу и позвоните по номеру с официального сайта организации.

Фарминг – более продвинутая версия фишинга, заключающаяся в переводе пользователей на фальшивый веб-сайт и краже конфиденциальной информации. **Цель** - получить персональные данные пользователей, но не через почту, а прямо через официальные веб-сайты. Этот вид мошенничества еще опаснее, так как заметить подделку практически невозможно.

Социальная инженерия. Это метод фишинга без использования специальных технических средств. Мошенник никого не взламывает, не подсаживает вирус и не перехватывает трафик. Все данные человек выдает сам— под действием обмана, угроз и манипуляций.

КАКИЕ БЫВАЮТ МЕТОДЫ ФИШИНГА?

Фишинговые ссылки — сообщение электронной почты содержит ссылку на страницу, похожую на страницу авторизации доверенного сайта и призывающую, например, срочно поменять пароль. Этим действием вы можете передать его непосредственно в руки злоумышленников. Задача мошенника — убедить получателя письма или сообщения, что нужно перейти по присланной ссылке.

Фишинговые сайты — это поддельные сайты госорганов, банков, популярных социальных сетей, маркетплейсов и других компаний. Они похожи на оригиналы внешне, но у них неправильное доменное имя. Например, вместо «online.sberbank.ru» написано «onllinesberbank.ru».

Фишинговые приложения. Мошенники размещают их в официальных онлайн-магазинах, проплачивают рекламу в других онлайн-проектах, а при скачивании или переходе по ссылке выводят на поддельные страницы, замаскированные под официальные ресурсы крупных компаний или СМИ, дублирующие их корпоративные цвета, шрифты и логотипы. Уже на этих ресурсах жертву обрабатывают, предлагая инвестировать деньги в якобы специально созданные финансовые структуры и обещая неслыханную и гарантированную доходность.