



Прокуратура Симферопольского района информирует

Виды онлайн-мошенничества

Фишинг – рассылка поддельных электронных писем и СМС или сообщений в мессенджерах, имитирующие коммуникацию от банков, государственных органов или известных компаний

Защита: проверка домена отправителя, использование двухфакторной аутентификации

Скимминг – установка вредоносных устройств (скиммеров) на банкоматы или создание поддельных сайтов для кражи данных карт

Защита: использование виртуальных карт для онлайн-платежей, блокировка подозрительных транзакций





Прокуратура Симферопольского района предупреждает

Виды онлайн-мошенничества

Мошенничество в социальных сетях – создание аккаунтов от имени знакомых или знаменитостей для вымогательства денег; ложные розыгрыши с требованием оплаты для получения «приза»; «любовные» аферы, шантаж-угрозы опубликовать личные фото/видео

Защита: ограничение доступа к личной информации, проверка подлинности аккаунтов

Финансовые пирамиды и инвестиционные схемы – псевдо-инвестиционные платформы, обещающие высокую доходность

Защита: проверка лицензии компании, анализ отзывов





Прокуратура Симферопольского района предупреждает

Виды онлайн-мошенничества

Мошенничество в онлайн-покупках – продажа несуществующих товаров на аукционах, маркетплейсах или через социальные сети

Защита: использование безопасных способов оплаты (эскроу), проверка рейтинга продавца

Вредоносное ПО и программы-вымогатели – вирусы, блокирующие доступ к данным до выплаты выкупа.

Защита: регулярное обновление ПО, резервное копирование данных





Прокуратура Симферопольского района предупреждает

Виды онлайн-мошенничества

Мошенничество с поддельными приложениями — вредоносные приложения, маскирующиеся под легальные сервисы (банкинг, доставка)

Защита: скачивание приложений только из официальных источников

Своевременное информирование и правовая осведомленность – ключевые инструменты противодействия киберпреступности!!!

