ИНТЕРНЕТ-МОШЕННИЧЕСТВО —

один из способов незаконного получения личных данных (паролей, реквизитов банковских карт) путем предоставления человеку неверной информации, фиктивных угроз, вымогательства

Самые распространенные схемы мошенничества:

- Обзвон граждан от имени правоохранительных органов или банков
- Создание фальшивых (фишинговых) сайтов для получения доступа к конфиденциальным данным пользователей
- Рассылка писем о «крупном выигрыше» по электронной почте
- Фальшивые сайты благотворительных организаций/туроператоров/ авиакомпаний
- Предложение выгодного заработка на подозрительных интернет-ресурсах
- Взлом личных аккаунтов пользователей и рассылка сообщений
- Лотереи, викторины, конкурсы, где нужно заплатить «налог на выигрыш» или «комиссию за доставку приза»

ПРАВИЛА ЦИФРОВОЙ ГИГИЕНЫ

- Не давайте свой телефон незнакомым людям под предлогом срочного звонка
- Устанавливайте длинные и надежные пароли, усиленные биометрией и двухфакторной аутентификацией. Регулярно меняйте их
- Устанавливайте оригинальные пароль, PIN-код и другие виды защиты для блокировки компьютера и телефона
- Выполняйте регулярное резервное копирование данных на внешний жесткий диск
- Избегайте публикации личной информации в соцсетях (номер телефона, фото, домашний и рабочий адреса, номера кредитных и банковских карт, местоположение)

ПРАВИЛА ЦИФРОВОЙ ГИГИЕНЫ

- Не принимайте заявки в соцсетях от незнакомых и сомнительных людей
- При установке нового приложения проверяйте, к каким данным на вашем устройстве у вас запрашивают разрешение
- Регулярно обновляйте программы, приложения и операционные системы. Старые версии могут быть более уязвимы для атак
- Отписывайтесь от ненужных рассылок и подписок
- Внимательно открывайте электронные письма с неизвестных адресов, не переходите по объявлениям и ссылкам, которые обещают скидки, призы и денежные выигрыши

ПРАВИЛА ЦИФРОВОЙ ГИГИЕНЫ

- При использовании публичных сетей Wi-Fi будьте аккуратны при открытии мобильного банка. Злоумышленники часто используют такие сети в своих целях
- Контролируйте покупки в интернете. Под видом онлайн-магазина могут быть мошенники
- Используйте сетевой экран. Он предотвращает несанкционированный доступ к вашим веб-сайтам, почте, паролям и другой информации
- При продаже старых гаджетов отформатируйте и очистите жесткий диск
- Используйте хорошее антивирусное программное обеспечение, регулярно проводите автоматическую проверку устройства на вредоносные программы

ОБЩИЕ РЕКОМЕНДАЦИИ

- Доверяйте только проверенным источникам
- Дайте новостям время: перепроверяйте информацию, добытую «по горячим следам»
- Проверяйте факты самостоятельно в нескольких авторитетных и официальных источниках
- Следите за порталами, которые раскрывают фейки и сообщают о них
- Проверяйте видео на дипфейки: следите за артикуляцией говорящего и его мимикой. При любом несовпадении проверьте данную информацию