**ПАМЯТКА ПО ЛИЧНОЙ**

**ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Число ИТ-преступлений в России за 2023 год выросло на 30%.

Мошенники украли у россиян почти 16 миллиардов рублей за год.

91% граждан сталкивались с попытками мошенничества.

Люди теряют средства не только через телефонное мошенничество. Преступления с использованием интернета продолжают расти из года в год.

Обмануть можно практически любого, а антивирусы не защищают нас от вредоносных программ на 100%. Поэтому, соблюдая несколько базовых правил цифровой гигиены, вы можете значительно усложнить жизнь мошенникам и киберпреступникам, сохранив свои средства в целостности.

**Защита от телефонного мошенничества**

- При любом звонке от банка, государственных ведомств и любых других организаций, если тема для разговора связана с какими-то проблемами с вашими деньгами, паролями, персональными данными, кодами, картами, кредитами, опасностью, помощью - прощайтесь с абонентом. Далее, найдите официальный номер телефона организации и узнайте у них, настоящий ли сотрудник вам звонил.

- Помните, номер телефона звонящего, который вы видите на экране, может быть подделан.

- К SMS и сообщениям в мессенджерах относитесь так же, как к звонкам. В случае сомнений найдите официальный телефон организации и перезвоните.

- Установите приложение с определителем номера (Яндекс, Касперский и т.д.).

- В банковском приложении установите суточный лимит на переводы средств. После этого увеличить его можно будет только через звонок в банк.

- Никогда не переводите средства по просьбам от незнакомых людей. Если просьба пришла от знакомого, свяжитесь с ним по другому каналу связи. Не торопитесь, деньги должны приходить быстро, а уходить медленно.

**Приготовьтесь к утере телефона**

- Поставьте ПИН-код на SIM-карту.

- Включите функцию «Найти устройство» или «Найти iPhone».

- Используйте пароль для входа в устройство (цифровой, графический, отпечаток пальца, Face ID).

- Удалите чувствительные данные на карте памяти: фото личных документов, файлы с работы и любую информацию, которая может вас скомпрометировать.

- Отключите отображение входящих смс на заблокированном экране.

**Безопасность SIM-карты:**

- Напишите заявление у своего сотового оператора, чтобы без вашего личного присутствия SIM-карту нельзя было переоформить на другого человека.

 - Заведите отдельную SIM-карту для «чувствительных» сервисов (банки, Госуслуги и т.п.).

**Безопасность паролей**

- На сайтах с важной и конфиденциальной информацией используйте разные пароли.

- Забудьте о простых паролях. Qwerty123 - слишком легкий пароль для злоумышленников. G!hsYuL2g^ - более подходящий.

- На важных сайтах включайте двухфакторную аутентификацию в настройках. Простыми словами – это двойной способ проверки. Такую проверку проводят различные сервисы в интернете, чтобы убедиться, что это действительно вы хотите войти в аккаунт (кабинет).

- Используйте специальные программы - менеджеры паролей, для хранения личных данных, например, Bitwarden, Keepass, Lastpass.

- Когда вводите пароль на телефоне и компьютере или ПИН-код в банкомате, обратите внимание, что за вами никто не наблюдает (в том числе видеокамеры). Прикройте вводимый код второй рукой.

**Безопасность смартфона и компьютера**

- Не выключайте функцию автоматического обновления программ.

- Скачивайте приложения на смартфон только с официальных магазинов App Store и Google Play. Не качайте приложения на неизвестных сайтах.

- Не разрешайте приложениям лишние функции, скачиваемому калькулятору не нужен доступ к вашим контактам.

- В официальных магазинах могут быть размещены мошеннические приложения. Читайте отзывы о приложении, особенно отрицательные.

**Безопасность персональных данных**

- Различные сервисы, могут попросить подтвердить свою личность с помощью фотографии, где будут видны ваше лицо и паспорт. Когда вы делаете подобные снимки, свободными пальцами или второй рукой держите надпись с названием компании, в которую вы отправляете фотографию. Злоумышленники воруют такие снимки тысячами и им легче удалить вашу фотографию, чем пытаться стереть название компании.

- На сайтах с розыгрышами, выгодными инвестициями и другими способами быстро разбогатеть или получить что-то в подарок не нужно оставлять свои персональные данные. Ваши ФИО и номер телефона как минимум продадут за $0,5 черным маркетологам, а в 95% случаев мошенникам.

- Не выкладывайте фотографии и сканы документов, подтверждающих личность, в социальных сетях, даже в личных сообщениях.

**Безопасный интернет**

- В публичных местах, если вы подключились к бесплатному WiFi – не вводите пароли даже на известных и доверенных сайтах.

- Не доверяйте всем QR-кодам, которые видите. QR код- «от англ. QR - Quick Response - Быстрый Отклик» — это штрихкод, предоставляющий информацию для ее быстрого распознавания с помощью камеры на мобильном телефоне. Проверьте, не наклеен ли поверх одного кода другой.

- Некоторые сервисы в интернете предлагают выбрать секретный вопрос и написать ответ на него. Пишите несоответствующие данные. Например, выберите вопрос "Индекс родителей", а ответ напишите «Барсик».

- В социальных сетях и мессенджерах лучше не открывать ссылки от незнакомцев.

- Даже ваших знакомых могут взломать, так что, если они вам прислали ссылку без объяснения или с подозрительным объяснением, лучше ее не открывать или проверить, действительно ли это ваш знакомый.

- Проверяйте ссылку не только перед переходом по ней, но и когда вы уже перешли на сайт. Сайт, на который вы попали, может отличаться от того, что было написано в ссылке.

- Если после перехода по подозрительной ссылке у вас запрашивают конфиденциальную или личную информацию, предлагают скачать файл – уходите с сайта.

Помните золотое правило защиты от киберпреступников и мошенников: если вас просят сделать действие, ищите подозрительные признаки.