РАССКАЖИ БАБУШКЕ

социальная кампания по финансовому просвещению старшего поколения

*за права заемщиков

НАРОДНЫЙ ФРОНТ

АССОЦИАЦИЯ РАЗВИТИЯ ФИНАНСОВОЙ ГРАМОТНОСТИ

Информационная безопасность для старшего поколения

telltogranny

telltogranny.ru

Интернет даёт массу возможностей.
Можно общаться, работать, учиться, смотреть кино
и телепрограммы, слушать музыку, искать информацию.
Однако в цифровой среде таится немало опасностей.

В интернете орудуют мошенники, которые могут
попытаться проникнуть в ваш компьютер или смартфон,
чтобы получить персональные данные или похитить деньги.
Внедрившись в вашу систему, они также могут
от вашего имени рассылать письма или совершать атаки
на других пользователей.

Для защиты установите на компьютер, а также смартфон
или планшет антивирусную программу и следуйте
технике информационной безопасности.

1. Электронная почта

Электронная почта позволяет обмениваться письмами с людьми по всему миру. Вы можете отправить документ, фото или видео безо всяких конвертов и марок. Послание будет доставлено моментально и бесплатно - очень удобно.

Чтобы переписка в интернете вам не навредила

1) Не открывайте письма от незнакомых отправителей и не переходите по ссылкам из них.

2) Для доступа к вашему электронному почтовому ящику нужен надёжный пароль, который злоумышленникам будет сложно взломать.

- Пароль должен состоять из 8-12 символов. Чем длиннее, тем лучше.

- Не используйте в пароле своё имя или имена родственников, клички домашних животных, номер телефона, адрес или дату рождения.

- В пароле должны быть строчные и прописные буквы, цифры, знаки препинания и другие символы - чем хитрее комбинация, тем безопасней. **Так выглядят удачные пароли bKriH)23bmWv или j5NTr93BmSeI4.** Сложный пароль можно создать при помощи специального приложения - генератора паролей.

3) **Не храните ваши пароли на компьютере.**
Лучше запомнить или записать их в блокнот.

4) Не используйте один и тот же пароль для разных сайтов и приложений.

5) **Каждые полгода обновляйте пароли.**

6) Время от времени проводите ревизию почтового ящика и отписывайтесь от ненужных рассылок и подписок. Они не только захламляют почту, но и могут быть платными.

7) **Остерегайтесь фишинга!**
Это уловка, при помощи которой мошенники пытаются получить доступ к данным пользователя, например, данным банковской карты или паролю от почты.

Жертва получает письмо или сообщения от адресата, которому доверяет: это может быть банк, любимый магазин, Социальный фонд или «Госуслуги». Человека просят срочно пройти по ссылке и указать или обновить личные данные, иначе у него возникнут проблемы. Это и есть «забрасывание удочки». **Если жертва пройдёт по ссылке и оставит там данные, они попадут к злоумышленникам.**

2. Как защитить аккаунт от мошенников

В интернете миллионы сайтов, и некоторые из них могут представлять опасность. **Поэтому стоит понимать, как определить сайты, заслуживающие доверия.**

- Если вы ищете сайт через «Яндекс», обращайте внимание на знаки около названия.
Например, белая галочка на синем фоне - признак надёжного сайта, такие есть у госучреждений, банков, сервисов самого «Яндекса» и др. А белый огонёк на зелёном фоне - метка популярного сайта с постоянной аудиторией, например, крупных СМИ и сайтов известных брендов.

- Тщательно проверяйте адреса сайтов, где собираетесь оставить свои данные. Мошенники маскируют вредоносные ресурсы под официальные, различаться может один символ. Например, частая уловка мошенников - заменить букву I на цифру 1.

2. Как защитить аккаунт от мошенников

- Сайты, название которых начинается с букв «https» и изображения замочка, считаются более защищёнными, чем те, у которых в начале «http».

- Не проходите по рекламным ссылкам из всплывающих окон. В интернет-браузере можно настроить блокировку рекламы. Это снизит вероятность случайно нажать на вредоносную ссылку.

- Мошенники активно создают поддельные фишинговые сайты, похожие на сайты настоящих магазинов, компаний, банков и пр.

Злоумышленники подделывают логотип, используют те же цвета и дизайн, что у оригинала. Распознать фейк можно при помощи специальных сервисов. Например, в приложении Сбера есть раздел **«Проверка сайтов».** Достаточно вставить там подозрительную ссылку и сервис сообщит, безопасно ли по ней переходить.

3. Соцсети и мессенджеры

Люди всё активней общаются онлайн, используя для этого социальные сети и мессенджеры.

Мессенджеры – это популярные приложения, в которых можно быстро обмениваться сообщениями, фото, видео. **Это WhatsApp, Viber, Telegram, «VK Мессенджер» и другие.**

Социальные сети, такие как **«Одноклассники», «ВКонтакте», объединяют миллионы людей.** Благодаря им можно найти старых и новых друзей, общаться с единомышленниками, обмениваться фотографиями и др.

Но не стоит забывать, что сетевое общение отличается от реального. Здесь есть свои нюансы.

- Не публикуйте в соцсетях лишней информации. Например, номер телефона, точный адрес, а также информацию о своих планах, например, о том, что вы собираетесь уехать на несколько дней. Эти сведения мошенники могут использовать против вас.

- Не выкладывайте сомнительные фотографии или посты, которые можно использовать против вас.

3. Соцсети и мессенджеры

- Недопустимо публиковать фото документов и банковских карт. Вы рискуете, что они окажутся у злоумышленников. А если документы чужие, это и вовсе преступление.

- Внимательно относитесь к виртуальным собеседникам, которых не знаете лично. Под чужим именем и фото может скрываться злоумышленник.

- Критично относитесь к сообщениям, полученным в мессенджерах и соцсетях, даже если получили их от знакомых. Если вас срочно просят помочь - не пугайтесь. Аккаунт ваших близких могли взломать. Прежде чем переводить им деньги попробуйте связаться с ними другим способом.

- Обезопасьте ваши мессенджеры от взлома - установите дополнительную проверку для входа в аккаунт. От вас кроме пароля потребуется код из СМС или отпечаток пальца, это существенно усложнит кибермошенникам взлом.

Следуйте правилам цифровой гигиены и пусть ваш серфинг в интернете будет безопасным!