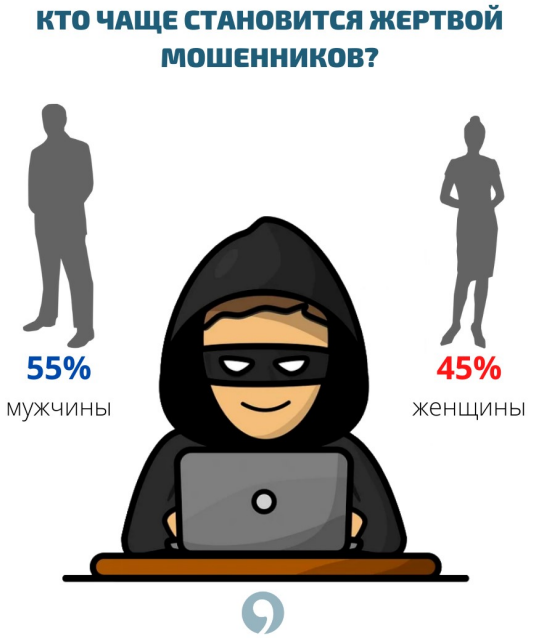
С каждым годом мошенники придумывают всё более изощрённые способы обмана, играя на доверии граждан к официальным инстанциям. В 2025 году мошенники начали использовать новые схемы, которые выглядят особенно правдоподобно. Разберём две свежие аферы и расскажем, как себя обезопасить.



других, содержащих конфиденциальную информацию.

Проверка надежности сайта. Обычный сайт защищен SSL-сертификатом, его адрес начинается с букв https, а в адресной строке появляется значок замка.

Отказ от переходов по незнакомым (подозрительным) ссылкам. Сюда относятся ссылки из спам-сообщений, приглашения в онлайн-викторины, кликбейтные заголовки, якобы бесплатные предложения. Сейчас в большинстве крупных почтовых сервисов стоит проверка писем, и система предупреждает пользователя о подозрительных ссылках. Также потенциальный спам уходит в специальную корзину. Но это происходит не всегда, а мошеннических ссылок в интернете великое множество.

Защита устройств. Большинство пользователей используют мобильные устройства3 для поиска информации и онлайн-покупок. Здесь также можно установить антивирус, использовать секретные коды и никому их не передавать, подключить биометрию.

Загрузка файлов из интернета. Скачивать программы лучше только с официальных сайтов – так ниже риск установить вредоносную программу, которую часто маскируют под популярные игры или иные приложения.

12+

**Центральная районная библиотека
МБУК «Велижская ЦБС
Центр правовой информации**

Осторожно! Новые формы мошенничества!

ВЕЛИЖ 2025

Новые формы мошенничества в сети

Звонок от «помощника судьи»

Мошенники представляются сотрудниками суда и звонят гражданам, называя якобы реальное дело (например, «по иску такого-то к такому-то»). Затем сообщают о назначении судебного заседания и просят подтвердить явку или согласие на рассмотрение дела без участия гражданина. Чтобы подтвердить решение, мошенники требуют назвать код из поступившего смс.

На самом деле этот код — подтверждение смены пароля от личного кабинета «Госуслуг». После его ввода злоумышленники получают доступ к аккаунту жертвы, включая её персональные данные, и могут взять кредиты на её имя.

Как не попасть в ловушку:

Помните, что сотрудники суда никогда не запрашивают коды из смс. Проверяйте информацию о назначенных заседаниях на официальных сайтах судов или через «Госуслуги».Если вам поступил такой звонок, не предоставляйте никакой личной информации.

Мошенники начали массово обманывать школьников и их родителей от имени учителей

Они создают дипфейк преподавателя и звонят, заявляя, что им надо обновить электронный журнал. Далее аферисты просят код из SMS и взламывают Госуслуги, а затем берут на родителей многомиллионные кредиты.

Пример: В МО МВД России «Белозерский» обратилась гражданка Н., у которой через мессенджер «WhatsApp» неустановленное лицо похитило 820 000 руб. Женщина подавала заявку в «Энергосбыт» на замену электросчетчика. Спустя несколько дней, ей поступил телефонный звонок через мессенджер «WhatsApp». Звонивший представился сотрудником компании «Энерго». В ходе беседы, потерпевшая сообщила свои персональные данные, в том числе паспортные. В этот же день, через мессенджер «WhatsApp», ей поступил телефонный звонок. Звонивший, представился сотрудником ФСБ и сообщил, что с ней беседовали мошенники, которые открыли на ее имя несколько кредитных обязательств в разных банках и предложил свою помощь. Чтобы «погасить» данные долги, ей необходимо, сделать переводы на другие счета, которые лжесотрудник ФСБ откроет на ее имя. На следующий день женщине снова позвонили через мессенджер «WhatsApp» и потерпевшая в течении дня сделала несколько переводов через банкомат ПАО «Сбербанк» на разные банковские карты на сумму 820 000 рублей, причем, мошенники все время оставались на связи, советовали ей периодически выходить из помещения банка, ни с кем не общаться, чтобы не привлекать внимания. **Граждане будьте бдительны! Не отвечайте на незнакомые номера, а если ответили, не называйте свои данные, ИНН, паспорт, СНИЛС, не сообщайте код из СМС, не переходите по ссылкам и позвоните в полицию! Ваша безопасность — в ваших руках!**

Общие правила и технические рекомендации по безопасности в интернете

Создание сильных паролей. Простые комбинации злоумышленники подбирают при помощи специальных программ. Если один и тот же пароль стоит на нескольких учетных записях, то данные подвергаются еще большему риску, потому как можно вскрыть все аккаунты и собрать про вас максимум информации.

Существуют программные менеджеры паролей и аутентификаторы, необходимо только найти продукт от надежного разработчика.

Подключение многофакторной аутентификации. Это метод верификации пользователя двумя и более способами. Например, помимо традиционной пары «логин-пароль» пользователь также должен ввести дополнительный одноразовый пароль из SMS, электронной почты, специализированного приложения, либо ответить на вопросы системы, предоставить отпечаток пальца, пройти распознавание по лицу.

Регулярные обновления программ и антивируса. Разработчики постоянно отслеживают последние угрозы и выпускают обновления безопасности, которые лучше устанавливать сразу. Особенно это касается приложений интернет-банков и