В настоящее время в России, как и во всем мире, продолжается процесс цифровизации и внедрения новых средств связи и удаленной коммуникации.

Помимо очевидных благ, данный процесс неизбежно сопровождается рисками, связанными с использованием преступниками современных технологий. Уровень киберпреступности на территории страны, не смотря на принимаемые правоохранительными органами меры, остается на достаточно высоком уровне.

Практически половину преступлений в мировой паутине составляют мошенничества, связанные с использованием средств мобильной связи или сети «Интернет».

Согласно данным ГУ МВД России по Воронежской области за 4 месяца 2025 года жители Воронежской области перевели мошенникам более 323 млн. руб.

Наиболее распространенным способом интернет-мошенничества при этом является «фишинг».

**Что же такое фишинговый сайт?**

Фишинговый сайт – это платформа для интернет-мошенничества, на которой злоумышленник получает доступ к конфиденциальным данным граждан, таким как логины и пароли, номера и коды безопасности кредитных карт.

Наибольшей популярностью у мошенников пользуется создание поддельных сайтов социальных сетей, банковских и финансовых организаций, учреждений, осуществляющих продажу товаров и услуг, организаций, оказывающих государственные услуги, принимающих оплату штрафов, налогов, услуг ЖКХ.

Интернет-шопинг – это, безусловно, удобно, но, к сожалению, и опасно.

Так, в 2024 году злоумышленникам удалось совершить 1,2 млн. успешных операций, по результатам которых у граждан было похищено 27,5 млрд. руб.

При этом благодаря работе банковской системы России было отражено 72,17 млн. попыток похищения денежных средств россиян., размер сохраненных денежных средств составил 13,5 трлн. руб.

Низкая финансовая грамотность интернет-покупателей - это то, чем так успешно пользуются киберпреступники.

**Как же обезопасить себя в случае оформления покупки в онлайн-магазине?**

Для этого надо придерживаться следующих общих правил поведения в сети «Интернет»:

1. Совершать покупки и заходить в свой онлайн-банк только с личных гаджетов (мобильных устройств и компьютеров), с установленными на них предварительно паролями.

2. Исключить случаи пользования общедоступными сетями Wi-Fi с устройств, имеющих доступ к Вашему банковскому счету (например мобильным телефоном имеющим приложение онлайн банка).

3. Выбирать сайты только с безопасным соединением и всегда внимательно проверять адресную строку браузера.

4. Выбирать известные интернет-магазины и сервисы. Добросовестный продавец всегда предоставляет полную информацию, свой телефон, адрес и другие важные данные.

5. Использовать систему безопасных платежей. Если онлайн-магазин поддерживает эту технологию, то после ввода реквизитов карты он перенаправит покупателя на безопасную интернет-страницу банка.

6. Завести отдельную банковскую карту для онлайн-покупок.

7. Не сообщать персональную информацию банковской карты (ПИН-код и код проверки подлинности карты (CVV2/CVC2/ППК2) или интернет-кошелька (логин и пароль от своего аккаунта)

8. Подключить СМС-оповещение об операциях по карте. Так вы быстро узнаете о платеже, которой не совершали, и сможете быстро заблокировать карту.

**Что же делать если Вы обнаружили фишинговый сайт?**

Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации в целях противодействия мошенничеству в сети Интернет разработана информационная система мониторинга фишинговых сайтов «Антифишинг», предназначенная для автоматизации и повышения эффективности процессов сбора, систематизации, обработки, анализа и хранения сведений о фишинговых ресурсах и фишинговой активности на территории Российской Федерации.

В связи с этим, в случае выявления сайтов указанной категории целесообразно использовать электронную форму направления обращений, расположенную по адресу: [https://paf.occsirt.ru](https://paf.occsirt.ru/).

Помимо этого, соответствующее заявление в информационную систему можно направить через портал «Госуслуги», которые расположены по адресу: <https://www.gosuslugi.ru>.

Для того чтобы подать обращение через Госуслуги Вам необходимо авторизоваться в системе и перейти во вкладку «подача жалобы о вредоносном ресурсе».

В открывшейся форме жалобы укажите адрес и язык фишингового сайта, адрес, с которого вы перешли на сайт мошенников. Если его нет — продублируйте адрес фишингового сайта.

Дату, когда Вы обнаружили фишинговый сайт или отправляете жалобу, а также адрес Вашей электронной почты для связи.

После заполнения указанной информации Ваша жалоба будет направлена в ИС «Антифишинг».

Срок обработки поступившей жалобы осуществляется в течении суток, после чего на указанную Вами ранее электронную почту поступит уведомление о результатах рассмотрения жалобы.