Приложение 3

УТВЕРЖДЕНО
Приказ генерального директора
научного учреждения
«ОИЭЯИ – Сосны»
«29» 10 2026 №199

ПАМЯТКА
по кибербезопасности и противодействию мошенничеству в сети Интернет для работников научного учреждения «ОИЭЯИ – Сосны»

В связи с резким ростом числа киберпреступлений и изощренностью методов социальной инженерии, убедительно просим Вас соблюдать базовые правила цифровой и финансовой гигиены для защиты ваших личных средств и конфиденциальных данных. Существует два основных способа киберпреступлений которые используют злоумышленники:

1. Телефонное мошенничество («Вишинг») это сплав слов «voice» и «phishing», проще говоря, «голосовой фишинг», то есть попытка мошенников обманом выведать у жертвы какие-то конфиденциальные сведения по телефону. Чаще всего это код подтверждения.

Злоумышленники действуют следующим образом: Вам звонят в мессенджерах (Viber, Telegram, WhatsApp, иные мессенджеры) или на Ваш абонентский номер под видом сотрудников банков, Следственного комитета, милиции, медицинских учреждений, сервисных служб (например, обслуживание домофонов, ЖКХ, мобильные операторы), любой существующей или выдуманной организации. Могут назвать Ваши ФИО, адрес места жительства, поскольку информацию о физических лицах злоумышленники получают благодаря взлому различных организаций, предоставляющих услуги, где храниться информация о заказе. В 2026 году злоумышленники взломали систему сети пиццерий «ДОДОпицца», на сайте граждане вводили личные данные для доставки товара, абонентские номера для подтверждения заказа, после взлома вся информация оказалась у злоумышленников.

2. Поддельные сайты («Фишинг») суть метода заключается в принуждении опонента к переходу по ссылке от имени легитимной организации (банка, налоговой службы, популярного интернет-магазина и т. д.). В подобных случаях целью, зачастую, является овладение банковскими данными.

Злоумышленники действуют следующим образом: мошенники создают сайты, визуально неотличимые от оригинальных интернет-банкингов, почтовых сервисов, служб доставки (Белпочта, Европочта) или торговых площадок (Kufar). Ссылки на них присылают в мессенджерах или социальных сетях. Внимательно проверяйте адресную строку, мошеннические сайты используют измененные доменные имена, которые могут отличаться одним или несколькими символами. Данный вид мошенничества в основном используется якобы для продажи различных товаров, вам под предлогом оформления заказа, услуги или регистрации предоставляют доступ на мошеннический сайт, где вы самостоятельно вводите свои личные данные, так же Вам нужно помнить, что злоумышленники не всегда имеют цель завладеть Вашими денежными средствами, благодаря сайтам они могут получить удаленный доступ к вашим мессенджерам и с них совершать последующие правонарушения.

3. Защита личных данных

Не передавайте посторонним лицам, не вводите на сомнительных сайтах свои персональные данные иную любую личную информацию. Обладая информацией, преступники могут воспользоваться ей в своих интересах.

В настоящее время в глобальной компьютерной сети интернет функционирует сервис «Проверь.Бел» который предназначен для проверки аккаунтов на предмет их использования в противоправной деятельности. Сведения в указанном сервисе формируются на основании информации правоохранительных органов.

Механизм действий, в случае если в отношении Вас совершено киберпреступление?

Рассмотрим на примере мошенничества

1. Первое и универсальное правило – **не поддаваться панике**. Важно понимать, что существует целый комплекс доступных мер для противодействия такого рода хищениям, эффективность которых главным образом определяется **быстротой Вашей реакции**.

2. Если вы понимаете, что стали жертвой мошенничества, а злоумышленники получили доступ к вашим персональным данным, то немедленно **заблокируйте банковские карты**.

Заблокировать карту можно следующими способами:

- позвонить в круглосуточный контакт-центр обслуживающего банка (обычно номер указан на обороте пластиковой карты);
- позвонить напрямую в круглосуточную сервисную службу Банковского процессингового центра;
- через мобильный или интернет-банкинг;
- через SMS-банкинг;
- в отделении банка.

3. При наличии возможности необходимо «по горячим следам» **зафиксировать всю имеющуюся информацию** о злоумышленнике: скриншоты (веб-сайта, социальной сети, переписки), имена, адреса, информацию, озвученную в ходе диалога, иные характерные особенности. В дальнейшем такие сведения могут быть очень полезны для установления и **поиска виновных лиц**.

4.1. Сообщите в обслуживающий банк **о хищении денег**. На основании обращения банк проведет внутреннюю проверку, результаты которой также могут быть полезны для расследования инцидента, так же банк может «заморозить» перевод на некоторое время.

4.2. Рекомендуем также запросить **письменное подтверждение от банка** о противоправном выводе денежных средств с ваших расчетных счетов – эта информация поможет точнее определить размер имущественного ущерба от действий злоумышленников.

5. Не стоит думать, что раз вы не знаете ничего о злоумышленнике, то дело безнадежно. За время существования интернет-мошенничества правоохранительные органы выработали эффективные меры расследования подобных дел.

6. Также **не стоит отказываться от обращения в милицию** по причине небольшой суммы похищенных денег: любые сведения о злоумышленниках помогают в раскрытии преступлений. Вполне вероятно, что вы не единственная жертва противоправных действий.

Будьте бдительны! Мошенники искусно манипулируют чувствами страха, тревоги за свои сбережения и спешки. Помните, что безопасность ваших средств зависит прежде всего от Вашей осмотрительности.