Информация об основных способах совершения мошеннических действий с использованием сети Интернет.

**Покупки и платежи в Интернете: основные правила безопасности.**

Много лет пользователи во всем мире пользуются онлайн-платежами. На сайтах или в приложениях интернет-магазинов вам доступен весь ассортимент товаров с простым механизмом поиска и возможностью заказать их прямо на дом.

Однако, онлайн-услуги удобны не только для покупателей, но и для преступников!

**Внимание!**

Мошенники создают «зеркальные» сайты – копии реально существующих магазинов, используют всего лишь одну лишнюю цифру или букву, иные символы, похищают деньги или данные невнимательных пользователей.

Мошенники регистрируются в качестве продавца, предлагают товары, получают заказы на них. После того, как покупатель оплачивает товар, мошенник сообщает, что товар закончился. Покупателю возвращается уплаченная сумма, а взамен приходит ссылка на сторонний сайт, где этот товар можно приобрести по скидке. Если купить что-то на таком сайте, то вместо желаемого товара могут прислать бракованный или просто пустые коробки.

Ни одна компания не будет продавать свои товары по невыгодным ценам. Мошенники используют скидки и распродажи, чтобы заманить доверчивых пользователей на свои сайты.

**Правила безопасности при совершении покупок в сети Интернет**

1) При любой покупке в Интернете будьте бдительными, подробно и внимательно изучите сайт, его название и указанный адрес, сравните его с официальным названием той организации, где желаете купить товары и услуги.

2) Не переходите ни по каким случайным ссылкам.

3) Не оставляйте данные своей банковской карты на подозрительных сайтах.

4) Изучайте отзывы о продавце, внимательно смотрите, когда он был зарегистрирован на сайте, торговой площадке, проверяйте даты отзывов о нем. Договаривайтесь с продавцом об оплате при получении товара. Если продавец отказывается от такого условия, это может свидетельствовать о возможном мошенничестве.

5) Сохраняйте всю переписку и контакты продавца, запишите название сайта. Указанные сведения помогут правоохранительным органам поймать мошенников.

6) Нет никаких гарантий, что при онлайн покупке вы получите заказанный качественный товар. Внимательно проверяйте отзывы о таких «магазинах» в сети!

**Мошеннические схемы в социальных сетях**

Мошенники, взломав страницы ваших близких, друзей, знакомых, от их имени рассылают сообщения о том, что оказались в трудной ситуации, и просят занять денег. Любые деньги, которые вы отправите, поступают на банковские счета мошенников.

Лучшим решением в данном случае будет звонок вашим друзьям, близким, чтобы выяснить, какие у них проблемы и нужна ли им реальная помощь.

Будьте бдительны при общении в социальных сетях!

**Цифровое мошенничество с криптовалютой**

Криптовалюта — это специальная цифровая валюта, которая существует только в виртуальном виде.

**Фальшивые биржи**

Фальшивые биржи – это мошеннические копии реальных криптовалютных бирж, где пользователи продают и покупают криптовалюту. Как правило, мошенники подделывают мобильные приложения, но вы также можете встретить целые программы или сайты-подделки. Будьте осторожны, потому что некоторые фальшивые биржи очень похожи на оригинальные. Их цель – украсть ваши деньги.

Как правило, фальшивые биржи привлекают криптотрейдеров (людей, которые торгуют криптовалютой) и инвесторов, предлагая бесплатные криптовалюты, низкие цены, низкие комиссии на торговлю и даже подарки.

Мошенники создают учетную запись будто бы от лица человека, обладающего большим авторитетом в мире криптовалют. Затем они объявляют о фейковых раздачах через рассылки или личные чаты.

Чтобы избежать мошенничества на поддельной бирже, тщательно проверяйте адрес сайта, обращайте внимание на детали и соблюдайте правила защиты от интернет-мошенничества!

**Мошеннические раздачи**

Мошеннические раздачи используются для того, чтобы выманить у вас криптовалюту, предложив что-то бесплатно в обмен на небольшой взнос. Обычно мошенники просят вас отправить средства на некий кошелек, чтобы вы могли получить обратно бóльшую сумму (например, «отправьте 0.1 BTC и получите 0.5 BTC»). Но если вы переведете криптовалюту, то ничего не получите и больше никогда не увидите свои средства.

Никогда не участвуйте в розыгрышах, где вам нужно сначала отправить деньги. По условиям честных акций с вас не будут требовать средства!

**Вредоносные программы. Вирусы**

Вредоносные программы используют фактор перевода криптовалюты друзьям. Как обычно, мошенник отправляет вам адрес своего кошелька, чтобы вы могли скопировать его и вставить в специальное приложение. Однако, если на вашем устройстве установлен вирус, то вместо адреса кошелька своего приятеля, вы отправите деньги на адрес кошелька злоумышленника.

**Финансовые пирамиды**

Финансовые пирамиды – это инвестиционная стратегия, при которой прибыль предыдущим вкладчикам выплачивается за счет денег новых вкладчиков. Лучший способ избежать финансовой пирамиды – тщательно изучить криптовалюту, которую вы планируете купить. Если стоимость криптовалюты зависит от появления новых инвесторов, участников или вкладчиков, то, скорее всего, перед вами финансовая пирамида. Избегайте участвовать в таких покупках!

**Письмо из МФЦ: каким способом ещё взламывают аккаунты на Госуслугах**

Боитесь пропустить важную информацию от госоргана? На этом построена новая уловка мошенников.

Мошенник звонит, представляется сотрудником «Почты России» и сообщает, что вас ждёт письмо из Многофункционального центра. Для большего эффекта может добавить, что вам приходило уведомление, но вы его проигнорировали. Но шанс получить важное письмо ещё есть!

Чтобы послание дошло до адресата, нужно назвать — внимание — код из СМС. На самом деле он нужен, чтобы восстановить доступ к учётной записи на Госуслугах.

Также мошенники представляются сотрудниками правоохранительных органов либо сотрудниками технической поддержки портала Госуслуги и сообщают, что неизвестные лица пытаются зайти в личный кабинет указанного портала, и во избежание указанных действий необходимо сообщить код подтверждения, который поступит в СМС-сообщении. После того как вы сообщите указанный код, мошенники получают доступ к вашей учетной записи, после чего скачивают всю информацию, размещенную в ней, а также направляют заявки с целью оформления займов в микрофинансовых организациях.

**Напомним:**

- чтобы защитить свой аккаунт на Госуслугах, включите двухфакторную аутентификацию и уведомления о входе в личный кабинет;

- настоящие сотрудники государственных организаций не просят назвать код из СМС;

- если вы подозреваете, что кто-то посторонний мог зайти в ваш аккаунт на Госуслугах, срочно измените пароль и сообщите о своих опасениях техподдержке портала (а перед этим убедитесь, что звоните по официальным контактам).

**Компьютерные вирусы**

Вирусы часто маскируются под безопасные программы.

Вирусы имеют следующие вредоносные функции:

- Крадут персональные данные пользователя: выгружают данные из системы, включая логины и пароли, платежные данные, личные файлы.

- Замедляют работу устройств.

- Передают злоумышленникам все, что пользователь печатает на своей клавиатуре.

- Блокируют устройство с целью шантажа, а для разблокировки требуют перевести деньги на указанный счет.

- Используют ваш компьютер для майнинга – добычи криптовалюты.

Не надейтесь на добросовестность мошенников! Перевод денег по указанным данным не поможет разблокировать устройство.

**Как можно определить, что ваше устройство заражено вирусами?**

- Появление новых папок и файлов без вашего участия.

- Чрезмерный нагрев устройства.

- Внезапные отключения или перезагрузка устройства.

- Самостоятельный запуск программ, движение курсора мыши и т.п.

- Появление на устройстве новых программ или приложений, которые вы не устанавливали.

- Появление рекламных баннеров, уведомлений и всплывающих окон.

- Чрезмерный расход денег на телефонном счете, появление ненужных платных подписок или платных функций, которые вы не оформляли.

**Если ваш компьютер заражен вирусами, лучшим решением будет очистить его с помощью надежной антивирусной программы.**

**Меры предосторожности, которые помогут избежать заражения устройства вирусами:**

1. Установите антивирусное программное обеспечение. Даже бесплатные программы способны отслеживать работу вашего устройства и вовремя удалять вирусные программы в случае их появления.

2. Не скачивайте файлы из ненадежных источников или сомнительных веб-сайтов. Не открывайте письма, присланные с незнакомых адресов.

3. Регулярно делайте резервное копирование всех своих важных данных, чтобы в случае вирусной атаки их не потерять.

4. Если вирусы нанесли системе непоправимый ущерб, и у вас нет возможности установить и воспользоваться антивирусом – обратитесь к эксперту из сервисной службы по ремонту компьютеров или смартфонов.

**Личный пример**

Используйте собственную надежную мобильную сеть или Wi-Fi сеть с паролем. Избегайте подключения к ненадежным Wi-Fi сетям, таким как открытые сети в кафе или в других общественных местах.

**Телефонные мошенники!**

Когда мошенники звонят жертве, они пытаются обманом, манипуляцией или запугиванием заставить человека сделать то, что им нужно – перевести деньги или передать свои персональные данные.

**Популярные схемы мошенничества в ходе телефонных разговоров:**

1. Звонок от имени сотрудника банка, службы безопасности, бюро кредитных историй, оператора сотовой связи, правоохранительных органов, Центробанка или любой другой уполномоченной организации.

2. СМС с просьбой о помощи. Обычно СМС приходит от имени человека, который вам хорошо знаком – сестры или брата, ребенка или родителя, другого родственника. Вместо СМС мошенники могут позвонить, сказав, что ваш родственник попал в беду. Мошенники рассчитывают, что напуганная жертва не будет перепроверять информацию и не догадается перезвонить своему родственнику, чтобы уточнить, правда ли это.

3. Сообщение с просьбой перезвонить. На телефон приходит СМС, сообщение в мессенджере или даже письмо на почту от имени какой-либо организации.

**Внимание! Звонки, как и сообщения, могут поступить абсолютно с любого номера – настоящего номера банка, полиции, организации. Сегодня с помощью специальных программ можно подменить абсолютно любой номер.**

**Чего мошенники добиваются звонками:**

- Пытаются обманом заставить перевести деньги. Мошенники могут рассказать вам, что ваши средства в опасности, а для того, чтобы защитить их, необходимо перевести все на некий «резервный» счет, который откроют специально для вас. Разумеется, никакого резервного счета не существует. Если согласиться и сделать перевод, деньги отправятся к мошенникам.

- Пытаются получить персональные данные и другую ценную информацию. Вместо того чтобы заставить человека перевести деньги, мошенники могут узнать его банковские реквизиты и перевести все деньги самостоятельно.

- Пытаются получить доступ в мобильный банк. С этой целью мошенники могут, например, отправить вам СМС с кодом доступа и попросить вас сообщить его под любым предлогом.

- Обманом пытаются заставить установить вирусное программное обеспечение либо приложение удаленного доступа, которые или будет следить за вашим устройством, или предоставит мошенникам полный доступ к устройству.

**К сведению!**

На современных телефонах Android присутствует встроенная бесплатная защита от спама. Чтобы включить ее, откройте приложение «Телефон», нажмите на значок «Еще» (выглядит как три точки), выберите пункт «Настройки», затем «АОН и спам». Включите пункт «Фильтровать спам-вызовы». На телефонах «Apple» встроенной защиты от спама нет, однако можно загрузить приложения для фильтрации мошеннических и спам-звонков.

**Как можно обезопасить себя от телефонных мошенников?**

1. С осторожностью относитесь к звонкам с незнакомых номеров. Если есть возможность, лучше вообще не отвечать на них.

2. Будьте внимательны и с осторожностью относитесь к тому, что вам говорят по телефону незнакомые люди. Они могут рассказывать вам что угодно, что вы могли стать свидетелем преступления, что нужна ваша помощь для поимки мошенников, что у вас хотят украсть деньги со счета, что на ваше имя неизвестные пытаются оформить кредит, что по вашей банковской карте происходили финансовые операции в поддержку ВС Украины, что ваш родственник попал в ДТП и во избежание ответственности необходимо перечислить денежные средства либо передать их курьеру.

3. Не ведите с мошенниками разговоров. Если думаете, что вам позвонили мошенники – вешайте трубку и блокируйте номер.

4. Подключите функцию защиты от спама на телефон.