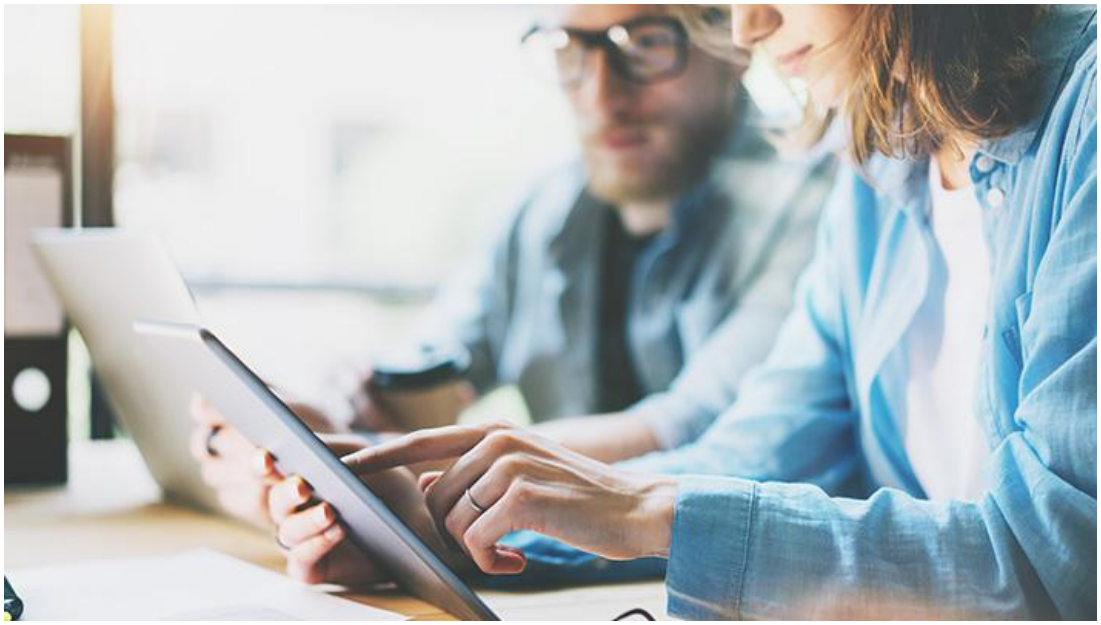
# Защита электронных денег в интернете



Поскольку совершать банковские операции и покупки в интернете очень удобно, все больше людей учатся использовать интернет в этих целях. киберпреступники пользуются этим для кражи паролей, персональных данных и денег покупателей.

***Советы по интернет-безопасности для защиты денег и кредитных карт***

Мы приводим несколько советов от экспертов в области интернет-безопасности «Лаборатории Касперского», которые помогут вам защитить ваши деньги и ваши данные при работе в интернете.

## Не доверяйте ссылкам

Если необходимо посетить интернет-банк, онлайн-магазин или веб-сайт для приема платежей, следует вручную ввести URL-адрес, а не проходить по ссылке. Не проходите по ссылкам в сообщениях в социальных сетях;

- ✓ Ссылки в e-mail-сообщениях
- ✓ Ссылки в сообщениях социальных сетей
- ✓ Сообщения в чатах
- ✓ Баннерная реклама на подозрительных сайтах
- ✓ Ссылки, пересылаемые незнакомцами

## Остерегайтесь фальшивых контактов

Добропорядочные финансовые организации никогда не присылают по электронной почте сообщения, в которых просят клиентов ввести личные данные во всплывающем окне.

- ✓ Отправлять личные данные по e-mail
- ✓ Посещать дополнительные сайты для авторизации
- ✓ Вводить персональные данные во всплывающем окне

## Проверьте URL-адрес

При посещении веб-страницы, на которой необходимо ввести конфиденциальные данные, внимательно проверьте, соответствует ли адрес страницы, отображаемый в браузере, странице, к которой вы намеревались получить доступ. Если URL-адрес состоит из случайного набора букв и чисел или выглядит подозрительно, не вводите никакие данные.

## Используйте шифрование

Всякий раз, когда требуется ввести конфиденциальные данные, проверяйте, используется ли соединение с шифрованием. Если соединение является безопасным, URL-адрес будет начинаться с букв «https», а в адресной строке или строке состояния браузера будет отображаться небольшой значок замка. Щелкните значок замка и внимательно просмотрите информацию о сертификате проверки подлинности SSL, который был выдан сайту. Таким образом можно узнать, когда сертификат был выдан, кто его выдал и на какой период.

## Используйте свой компьютер и свой выход в интернет

Постарайтесь не использовать компьютеры с общим доступом (в интернет-кафе, аэропортах, клубах, гостиницах, библиотеках и других местах) для входа в онлайн-банкинг или покупок в интернет-магазинах. Эти компьютеры могут быть заражены шпионскими программами. Если это так, эти вредоносные программы могут записывать все, что вы вводите на клавиатуре, включая пароли, а также перехватывать интернет-трафик.

Даже при использовании собственного компьютера для финансовых операций в интернете не следует подключаться к интернету по общедоступной сети Wi-Fi. В общедоступной сети Wi-Fi существует опасность перехвата трафика администратором сети или киберпреступниками, и с помощью сетевых червей могут быть запущены те или иные атаки.

## Не используйте свою основную кредитную карту или дебетовую карту

Рекомендуется завести специальную карту, которая будет использоваться только для покупок в интернете. Также можно попробовать ограничить лимит кредитования для «интерактивной кредитной карты» или зафиксировать ограниченную сумму на «интерактивной дебетовой карте».

## Опыт других людей поможет вам избежать ошибок

Прежде чем купить что-нибудь в интернете, попробуйте прочитать отзывы покупателей о том или ином интернет-магазине.

## Остерегайтесь потенциально ненадежных сайтов

Не рекомендуется совершать покупки в интернет-магазинах, веб-сайты которых зарегистрированы на бесплатных хостингах.

## Узнайте дополнительную информацию об этом веб-сайте

Если имеются какие-либо сомнения или подозрения по поводу веб-сайта интернет-магазина, используйте IP-службу «Whois» для получения дополнительной информации о домене, в том числе о том, как долго он используется и кто его владелец. Обратите внимание на период времени, которое оплачено доменом.

## Устраните уязвимости в операционной системе и приложениях

Всегда устанавливайте самые последние обновления для операционной системы и всех приложений на компьютере и других устройствах. Это поможет устранить уязвимости операционной системы и приложений, которые могут быть использованы вредоносными программами.

## Используйте сетевой экран

Кроме использования стандартного сетевого экрана, для дополнительной безопасности можно запустить сетевые экраны на основе приложений и программного обеспечения.

## Обеспечьте защиту от вредоносных программ в интернете

Надежное антивирусное решение может защитить ваш компьютер от вирусов, червей, троянских программ и т.п. В некоторых антивирусных продуктах используются специальные технологии, которые обеспечивают дополнительную защиту при совершении покупок в интернет-магазинах и входе в онлайн-банкинг.