ПАМЯТКА
по безопасности при осуществлении интернет-платежей

В целях повышения осведомленности и обеспечения безопасности интернет-платежей представлены наиболее популярные формы мошенничества в сети интернет и рекомендации по обеспечению безопасности.

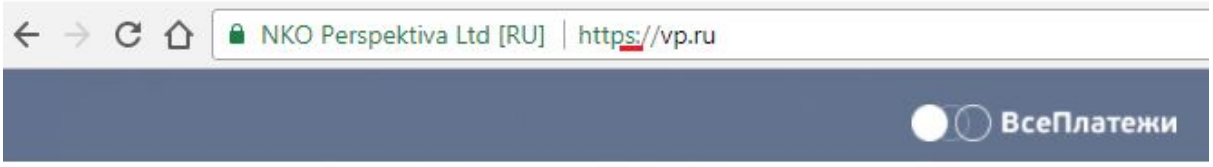
Фишинг (от англ. Phishing (password+fishing) - выуживание паролей) – это вид интернет-мошенничества, цель которого — получить конфиденциальные данные пользователей — логины и пароли, персональные данные, данные банковских карт и т.д. Достигается путем проведения массовых рассылок электронных писем от имени определенной компании.

Обычно такие письма приходят в виде уведомлений о каких-либо событиях (утеря данных, сбои в системе, получение бонусов за услуги, проведение лотерей и розыгрышей и т.д.), в связи с которыми пользователь должен предоставить, обновить или подтвердить те или иные конфиденциальные данные. При этом в письме приводится ссылка, которая ведет не на официальную страницу сервиса, а на ее точную копию. Информация, введенная пользователем на поддельном сайте, становится доступной мошенникам.

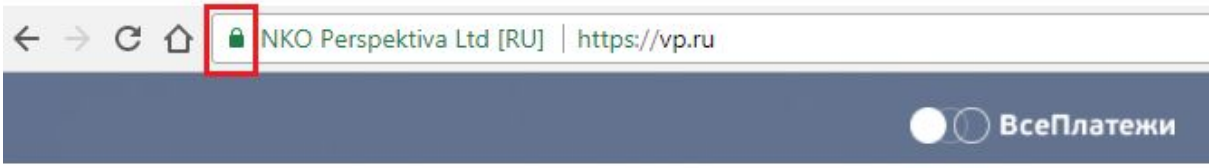
Как отличить настоящий сайт от поддельного?

1. Убедитесь в правильности написания адреса интернет-сайта в адресной строке браузера, проверьте на наличие незначительных ошибок в написании

2. Используйте лишь безопасные https-соединения. Отсутствие всего одной буквы “s” в адресной строке должно насторожить



3. Проверьте наличие значка “Замок” в браузере, такой значок означает, что у сайта есть сертификат безопасности (в зависимости от браузера “Замок” может быть расположен в правом нижнем углу веб-страницы или справа/слева от адресной строки)



Важно

Если вы под видом сервиса ВсеПлатежи получили сообщение на e-mail или sms с предложением перейти на сайт, отличающийся от vp.ru, или вам поступил звонок с просьбой сообщить пароль, данные банковской карты, одноразовый код безопасности для проверки данных или во избежание блокировки - не делайте этого!

Сотрудники платежного сервиса vp.ru никогда не запрашивают подобную информацию!

Максимальный набор информации, который может понадобиться сотрудникам сервиса ВсеПлатежи, чтобы найти ваш платеж в системе и предоставить информацию по нему - *первые 6 цифр и последние 4 цифр номера карты*. Все остальные данные о карте не сообщайте никому ни под каким предлогом!

Вредоносное программное обеспечение

Еще одним из распространенным способом хищении конфиденциальной информации является заражение компьютера пользователя вирусами.

Вирусы проникают на компьютер через интернет либо через письма рассылаемые под видом известных компаний. Ни в коем случае случае нельзя переходить по ссылкам и устанавливать приложения или обновления

безопасности, рассылаемые по e-mail или sms с незнакомых вам почтовых адресов или номеров телефона, в таком случае лучше связаться с отправителем любым другим доступным способом и уточнить факт отправки данного письма.

Основные правила, которые необходимо соблюдать при осуществлении интернет-платежей

1. Обязательно проверяйте URL-адрес на наличие незначительных ошибок в написании, устанавливайте соединение именно с официальным сайтом vp.ru ;
2. Используйте лишь защищенное соединение для обмена информацией: наличие значка “Замок” и https в адресной строке;
3. Никому не сообщайте ваш пароль, даже сотрудникам сервиса ВсеПлатежи;
4. В случае если возникли подозрения, что кто-либо получил доступ к вашему личному кабинету, смените пароль, либо обратитесь в службу поддержки клиентов по телефону +7 800 700 08 38;
5. Установите и регулярно обновляйте антивирусное программное обеспечение (например, Kaspersky, DrWeb и т.п.), и проверяйте компьютер, мобильное устройство на наличие вирусов и вредоносных программ. Так как действие вирусов может быть направлено на передачу третьим лицам вашей конфиденциальной информации;
6. Используйте sms-подтверждение платежей - 3D-Secure (3DS). 3DS служит дополнительным уровнем аутентификации пользователей при совершении платежей в Интернете. Предусматривает введение дополнительного кода подтверждения транзакции, который приходит на номер телефона в виде sms.
7. После окончания работы в личном кабинете обязательно нажимайте кнопку Выход.

Безопасность банковских карт

Рекомендуем вам ознакомиться с памяткой Банка России «О мерах безопасного использования банковских карт» в разделе Документы

Описанные в ней рекомендаций позволят Вам обеспечить сохранность денежных средств и минимизировать риски при совершении операций с использованием банковской карты.

Если вы стали жертвой мошенничества

Если с вашей карты были совершены мошеннические переводы денежных средства, которые вы не совершали, необходимо

- во-первых, немедленно обратиться в банк-эмитент, выпустивший карту, с которой произошло списание денежных средств с заявлением о мошеннической операции;
- во-вторых, передать информацию любым доступным способом - по телефону +7 800 700 08 38 , на электронную почту abon@vp.ru , в чате и др. специалистам службы поддержки клиентов сайта vp.ru;
- в-третьих, обратиться с заявлением в правоохранительные органы

В случае, если вам стала известна информация о том, что кто-то использует бренд vp.ru (товарные знаки или изображения) в противоправных целях, просьба сообщить специалистам службы поддержки клиентов сайта vp.ru (+7 800 700 08 38).