ООО НКО «ПэйЮ» РФ,
119002, г. Москва, ул. Арбат, д. 10.
Тел. +7 (499) 649-20-09
Email: info@payu.ru
www.nco-payu.ru

УТВЕРЖДАЮ
Исполняющий обязанности Председателя Правления
ООО НКО «ПэйЮ»
А.Б. Журавлева

18 апреля 2017 года

Рекомендации по защите информации от несанкционированного доступа путем использования ложных (фальсифицированных) ресурсов сети Интернет

Фишинг – это техника, благодаря которой осуществляется обман пользователя с целью кражи конфиденциальной информации, паролей и пр. Пользователь думает, что переходит на заявленный сайт, однако фактически его перенаправляют на подставной сайт. Очень часто подобного рода атаки производятся с помощью электронных писем. Данные электронные письма содержат ссылку, которая якобы ведет пользователя на сайт какой-то компании с высоким уровнем конфиденциальности, хотя, на самом деле, такой сайт – это всего лишь имитация оригинального сайта без какой-либо конфиденциальности. Таким образом пользователь может стать жертвой атаки, предназначенной для кражи персональных данных.

Чтобы защитить себя, необходимо следовать нескольким простым правилам:

1. Научитесь выявлять подозрительные фишинговые письма. Есть несколько признаков, которые идентифицируют атаку по электронной почте:
   - Они дублируют образ известной компании.
   - Они копируют название компании или ФИО реального сотрудника компании.
   - Они содержат сайты, которые визуально похожи на сайты реальных компаний.
   - Они предлагают подарки или пугают потерей существующего аккаунта.
2. Всегда внимательно проверяйте ссылку, по которой собираетесь кликнуть: не перепутаны ли буквы в названии сайта. Если с написанием что-то не так, это верный признак, что мошенники подсовывают вам поддельную страницу.
3. Проверяйте источник информации. Например, Ваш банк (да и любая другая организация) никогда не будет просить Вас отправить Ваши пароли или персональную информацию по электронной почте. Никогда не отвечайте на подобные вопросы, а если у Вас есть сомнения, то лучше позвоните в Ваш банк/организацию для получения разъяснений.
4. Перед тем как вводить логин и пароль, нужно проверить, защищено ли соединение. Если перед адресом сайта вы увидите префикс https (где «s» означает secure — безопасное), то все в порядке.
5. Даже если письмо или сообщение со ссылкой пришло от доверенного отправителя, все равно нужно помнить, что его тоже могли обмануть или взломать. Поэтому ведите себя не менее осторожно, чем при обращении со ссылками, пришедшими из неизвестного источника.
6. Старайтесь не нажимать ссылки в письмах. В результате этого Вы можете оказаться на подставном сайте. Лучше вручную наберите адрес сайта в адресной строке Вашего браузера или используйте ранее настроенную закладку в Избранном.
7. Используйте антивирусную программу, осуществляющую постоянный контроль компьютера или мобильного устройства. Запускайте периодическую полную проверку системы.
8. Регулярное обновляйте операционную систему, ее компоненты и антивирусное программное обеспечение с сайта производителя. Настройте автоматическое обновление.

Общество с ограниченной ответственностью небанковская кредитная организация «ПэйЮ».

ОГРН 1137711000082. ИНН 7750006806. КПП 775001001.

ОКПО 17410392. ОКАТО 45286575000. ОКВЭД 65.12. ОКОПФ 12165. ОКС 34

9. Иногда фальшивые письма и фальшивые сайты во всем повторяют дизайн настоящих. Качество подделки зависит от того, насколько хорошо преступники выполнили «домашнюю работу». А вот гиперссылки, скорее всего, будут неправильные — или с ошибками, или вообще будут ссылаться не туда. По этим признакам можно отличить фишинговое письмо от настоящего.
10. Обнаружив фишинговую операцию, крайне желательно сообщить о ней в банк (если письмо пришло от имени финансового учреждения) или в службу поддержки соцсети (если такие ссылки рассылает кто-то из пользователей) и так далее. Так вы поможете вовремя остановить мошенников.
11. По возможности не заходите в онлайн-банки и тому подобные сервисы через открытые Wi-Fi-сети в кафе или на улице. Лучше воспользоваться мобильным Интернетом или потерпеть, чем потерять все деньги на карте. Дело в том, что за таким Wi-Fi могут стоять мошенники, подменяющие адрес сайта на уровне подключения и перенаправляющие вас таким образом на поддельную страницу.
12. Лучший способ предотвращения фишинга – это не реагировать на любые письма или новости, которые просят Вас предоставить конфиденциальные данные. Удалите эти сообщения и позвоните в Ваш банк/организацию для прояснения Ваших сомнений.
13. Периодически читайте информацию о развитии вредоносных программ. Если Вы хотите быть в курсе последних вредоносных атак, рекомендаций или советов, чтобы избежать любых опасностей в Интернете, Вы можете читать специализированные блоги о кибер-безопасности в Facebook , ВК, Twitter и др.