Что такое фишинг и как защититься от кражи паролей в интернете?

Фишинг — это вид интернет-мошенничества, основанный на невнимательности пользователей в Сети. Чтобы вытянуть из пользователей личные данные, логины, пароли, номера банковских карт или другую важную информацию, злоумышленники создают поддельные страницы сайтов магазинов, банков, почтовых клиентов и соцсетей. Визуально они не отличаются от оригинальных, поэтому невнимательный посетитель вводит свои данные авторизации, после чего они попадают к мошенникам. Таким образом, мошенники могут взломать страницу вконтакте с помощью фишинга или получить доступ к банковскому аккаунту своей жертвы.

Как обеспечить защиту от фишинга?

Прежде всего, не доверяйте сообщениям, поступающим на вашу электронную почту, и не переходите по ссылкам, указанным в письме! Банки и соцсети не занимаются рассылкой по почте в случае проблем с аккаунтом. Никогда не вводите свои конфиденциальные данные на домены, начинающиеся с http:// (то есть незащищенные домены), следите, чтобы адрес сайта начинался с безопасного протокола https://.

Надежный способ защитить себя от фишинговой атаки - установить контент-фильтр SkyDNS. Благодаря нашему сервису вы можете быть уверены, что ваши личные данные и пароли не «утекут» к мошенникам.

Как проверить сайт на фишинг?

Не уверены в безопасности страницы? На сайте SkyDNS вы можете проверить сайт на фишинг:

1. Перейдите в форму проверки: https://www.skydns.ru/check/.
2. Скопируйте подозрительную ссылку и вставьте ее в нужное поле.
3. Сервис автоматически определит принадлежность сайта к той или иной категории.

Куда сообщить о фишинговом сайте?

Если вы обнаружили подозрительный сайт, отличающийся от оригинала внешне или в адресной строке, сообщите об этом:

- владельцу или администрации ресурса;
- support@skydns.ru. Мы включим сайт в список блокировки

Revision #5
Created 1 February 2024 07:29:36 by Виктор
Updated 29 May 2026 09:54:09 by Ольга