OUCH! Июнь 2023

OUCH!

SANS SECURITY AWARENESS

Ежемесячный информационный бюллетень по безопасности

Защита ваших финансовых счетов

Обзор

Ваши финансовые счета являются основной целью киберпреступников. У вас есть деньги, и они сделают все, чтобы их украсть. Под финансовыми счетами мы подразумеваем не только ваши текущие или сберегательные счета, но также инвестиционные, пенсионные и счета для онлайн-платежей, такие как PayPal. К счастью, с помощью нескольких простых шагов вы можете защитить себя.

Как они атакуют?

Банки вкладывают огромные средства в обеспечение безопасности своих систем, поэтому киберпреступникам крайне сложно их взломать. Вот почему киберпреступники вместо этого нацелены на вас и ваши учетные записи. Они знают, что у вас нет собственной службы безопасности, поэтому взломать вас гораздо проще, чем банк. Вот два наиболее распространенных способа, которыми они нацелятся на вас и попытаются украсть ваши деньги:

Пароли: каждый из ваших финансовых счетов защищен паролем. Если киберпреступник сможет угадать или скомпрометировать какой-либо из этих паролей, он сможет войти в систему как вы, а затем перевести ваши деньги на банковские счета, которые они контролируют. Есть множество способов, которыми они попытаются получить ваш пароль. Одним из распространенных способов является заражение вашего компьютера вредоносными программами. Как только ваш компьютер заражен, они могут заполучить ваше имя пользователя и пароль при доступе к веб-сайту вашего банка. Еще один распространенный метод — рассылка фишинговых писем, якобы отправленных из вашего банка. Когда вы нажимаете на ссылку в электронном письме, вы думаете, что входите на веб-сайт своего банка, но на самом деле вы входите на поддельный веб-сайт, который контролируется преступниками. Это позволяет им еще раз получить ваше имя пользователя и пароль, которые они затем могут использовать для входа в систему вместо вас.

Спрашивать: киберпреступники могут просто попросить вас ввести пароль или попросить перевести им деньги. Такие атаки социальной инженерии часто начинаются с того, что вы звоните по телефону. Киберпреступники знают, что как только они заставят вас говорить, им будет намного легче использовать эмоции, чтобы заставить вас совершить ошибку. Вот почему вы начинаете видеть больше фишинговых писем, голосовой почты и всплывающих окон браузера, которые создают ощущение срочности, сообщая вам, что вам нужно позвонить по номеру телефона, чтобы решить проблему или воспользоваться удивительной возможностью, прежде чем она истечет. Как только вы звоните по номеру телефона, преступники создают огромное давление, чтобы предоставить им доступ к вашим счетам, либо перевести ваши деньги на другие счета для них. Например, они могут сказать вам, что они из службы технической поддержки или правительства, утверждая, что ваш компьютер заражен и что, если вы не будете действовать сейчас, вы потеряете все свои деньги.

Как защитить себя?

К счастью, обеспечить безопасность ваших банковских счетов проще, чем вы думаете. Вот основные шаги, чтобы защитить себя:

1. **Будьте подозрительны**: прежде всего, вы являетесь самой лучшей защитой. Если вы получаете электронное письмо, текстовое сообщение, голосовую почту или всплывающее окно браузера, которое кажется странным или подозрительным, это может быть атакой. Чем сильнее чувство безотлагательности и чем сильнее вас заставляют действовать СЕЙЧАС, тем более вероятно, что это атака.

2. **Используйте надежные пароли/MFA**: Защитите каждую из ваших финансовых и личных учетных записей электронной почты с помощью длинного уникального пароля. Не можете запомнить все свои пароли? Подумайте об использовании менеджера паролей, чтобы надежно запомнить и сохранить их для вас. Лучший способ защитить каждую из ваших финансовых учетных записей — включить функцию многофакторной аутентификации (MFA) для каждой учетной записи.

3. **Контроль**: наконец, контролируйте все свои финансовые счета. Вы можете настроить автоматические оповещения, которые будут приходить вам по электронной почте или в текстовом сообщении каждый раз, когда деньги будут переведены на счет или сняты с него. Таким образом, вы можете быстро обнаружить любую несанкционированную или подозрительную транзакцию. Чем раньше вы обнаружите что-то не так и сообщите об этом в свой банк, тем больше шансов, что вы сможете вернуть свои деньги.

Приглашенный редактор

Линн Дом — исполнительный директор организации Women in CyberSecurity (WiCyS). От своего опыта работы в сфере образования в области кибербезопасности до активного участия в программах, финансируемых за счет грантов, и в некоммерческих организациях Линн распространяет информацию о важности диверсификации рабочей силы в области кибербезопасности.
Twitter: @lynn_dohm. Linkedin: https://www.linkedin.com/in/lynndohm/.

Ресурсы

Эмоциональные триггеры: как вас обманывают кибер-злоумышленники: https://www.sans.org/newsletters/ouch/emotional-triggers-how-cyber-attackers-trick-you/
Фишинговые атаки становятся все более изощренными: https://www.sans.org/newsletters/ouch/phishing-attacks-getting-trickier/
Менеджеры паролей: https://www.sans.org/newsletters/ouch/password-managers/
Многофакторная аутентификация: https://www.sans.org/newsletters/ouch/one-simple-step-to-securing-your-accounts/

Роман Полаков