



Reused Login Credentials

Security Advisory
February 2, 2010

Executive Summary

Internet users are required to memorize multiple login credentials to access different web services. As a result, many decide to use the same login credentials for multiple websites. This practice can be dangerous when sharing login credentials used for online financial services applications with less secure websites. Criminals have devised various methods to steal login credentials from less secure websites, which they then test them out on financial services websites. As a result, users are exposed to account hijacking risks which can lead to fraud.

Trusteer measured the magnitude of this problem, and discovered that:

- 73% of users share the online banking password with at least one nonfinancial website
- 47% of users share both their online banking user ID and password with at least one nonfinancial website.

Introduction

An average Internet user subscribes to multiple websites: online banking and other financial services, webmail services, social networks, newspapers, and more. Each of these websites requires registration and the use of login credentials, usually in the form of a username and password. As a result, a typical user needs to manage several and sometimes dozens of usernames and passwords.

To ease this burden, many users reuse the same login credentials on multiple websites. For example, users may use the same username and password for both their online banking application and their email account. Consequently, anyone who gets a hold of a user's email credentials can also use this information to access the user's online banking account.

Some websites enforce rules regarding the use of usernames and passwords. For example, some financial institutions choose usernames for their users; they do not allow users to choose their own usernames. To minimize the number of usernames to remember, users of these financial institutions reuse the assigned usernames on other websites, as well. On the other hand, many financial institutions allow their customers to choose their own usernames.

Some websites force users to change their passwords every few months. To handle this requirement, many users have a set of between three and five passwords that they use in rotation between all the different websites to which they subscribe.

Meanwhile, some users use password managers – tools that automatically fill out the correct username and password for each website. However, a tool that manages all of the usernames and passwords for an individual is a potential security threat. Criminals who hack into the computer can use the password manager to log onto any service that the user is registered to. Websites that aggregate usernames and passwords for users are even more dangerous. Once criminals obtain the login credentials to such a website, they can use it to log onto any other website as the authorized user.

How exactly do criminals take advantage of the fact that users reuse their login information on multiple websites? Below we explain some of the more common attack vectors.

Attacks on Shared Login Credentials

Website and Database Hacking

Websites usually store login information in a database. By hacking into the database, either directly or through the application, it is possible to obtain the login credentials of all users who are registered to the website.

However, hacking into a bank application or its associated database can be a complex task due to the various layers of security typically used to protect these assets. It is much easier to hack into a smaller non-financial website. The login credentials stolen from this website can be used later to compromise a user's online banking account and other accounts, assuming of course that some of these users share their login credentials with multiple websites.

An example of a recent database hack occurred at Suffolk County National Bank – a small New York bank. The bank's database was compromised in November 2009, and credentials for 8,378 online accounts were pilfered.

Brute Forcing and Password Recovery

Brute forcing refers to trying tens of thousands of possible passwords against a specific account until succeeding. Normally, banks do not allow you to brute force their accounts, and lock the attacked account after three to five unsuccessful logins.

However, some smaller and less secure websites do not have the same controls in place. If an attacker uses brute force to break into one of these websites, they can use the stolen login credentials on banking and other financial services websites.

Recovering a forgotten online banking password is not a pleasant experience. Banks must take extraordinary measures to properly authenticate a user before sending them new login credentials. This might not be the case for smaller and less secure websites. Some have less secure password recovery processes which criminals have learned to exploit. By exploiting these loopholes, criminals can obtain login information to these websites and try them with online banking applications.

One example of this password recovery mechanism exploit was the theft of a Twitter employee's Gmail account in 2009. You can read more about it at <http://www.scmagazineuk.com/hacker-croll-details-how-he-hit-gmail-account-of-twitter-employee-that-led-to-last-weeks-incident/article/140334/>

Phishing

Many users have learned to detect phishing messages that pretend to be sent on behalf of their bank. However, most are less likely to be suspicious of and capable of identifying phishing attacks masquerading as a message from a less significant service such as a newspaper subscription or Internet provider account?

These phishing attacks can serve two purposes – they can be used to steal login information and test it on additional accounts such as online banking applications. They can also be used to steal some personal information about the user from the phished account – information that can later be exploited to launch a more sophisticated attack against the individual.

Phishing attacks against nonfinancial websites in order to use them later for financial gain are becoming more popular. Facebook (<http://www.facebook.com/group.php?gid=9874388706>) and other

social networking websites are one of the primary targets, as they also store a lot of information about the victim. This information can be used to completely take over the victim's account when additional questions are asked (such as the name of the victim's dog, or the name of the victim's first school). The answers to most of these questions are on Facebook.

Untrusted Websites

Untrusted websites lure users to register for free services. These websites are either operated by criminals, or sell information to criminals. If a user logs into these websites with the same login credentials used for other services, criminals are able to gain control of online banking credentials.

All of these attacks, and others, rely on the fact that users are sharing their login credentials among multiple websites. But how common is this practice? Trusteer conducted research to find out.

Methodology

Trusteer's research is based on statistics gathered over a 12 month period from Rapport plug-ins running on more than 4 million computers. Rapport protects online banking and shopping customers from malware and phishing attacks.

One of Rapport's features warns users when they type their bank login information into other websites. This feature is used primarily to detect and block phishing attacks that lure users to submit their online banking login credentials to fraudulent look-a-like websites. However, this feature is also used for educational purposes; it lets users know that sharing their online banking login information with other websites is a security risk, and advises them to use different sets of login credentials for financial and nonfinancial websites.

For the purpose of this research, Trusteer gathered usage statistics from the above feature. Trusteer counted the number of customers who actually shared their online banking login information with nonfinancial websites.

Note: Rapport and Trusteer do not store or log customers' passwords and this information never leaves the customer's computer.

Login Credentials Reuse Statistics

Password Sharing

We found that 73% of users share the passwords which they use for online banking, with at least one nonfinancial website.

User ID Sharing

When a bank allows users to choose their own user ID, 65% share their banking username with nonfinancial websites.

When a bank enforces a unique user ID convention and chooses the user ID for the customer, 42% use the bank issued user ID with at least one other website.

User ID and Password Sharing

47% of users share both their user ID and password with at least one nonfinancial website.

Recommendations

For consumers:

- Remembering multiple usernames and passwords is challenging. Therefore, Trusteer recommends that users keep at least three sets of credentials: the first set to be used only with financial websites; the second set to be used with nonfinancial sensitive websites that hold information about your identity; the third set to be used with non-sensitive websites that do not maintain confidential information about the user. Memorizing three sets of credentials is not difficult, yet significantly improves a user's level of security.
- Although not immediately obvious, nonfinancial websites that store sensitive information about a user, such as webmail and social network accounts, can lead to financial fraud. Users should be diligent in safeguarding their login credentials to these websites.

For financial institutions:

- Identify customers who use their bank login information on nonfinancial websites and:
 - Educate them to avoid this risk

- Set your risk engine to higher sensitivity for these customers

* Both can be achieved with the Trusteer Rapport service.