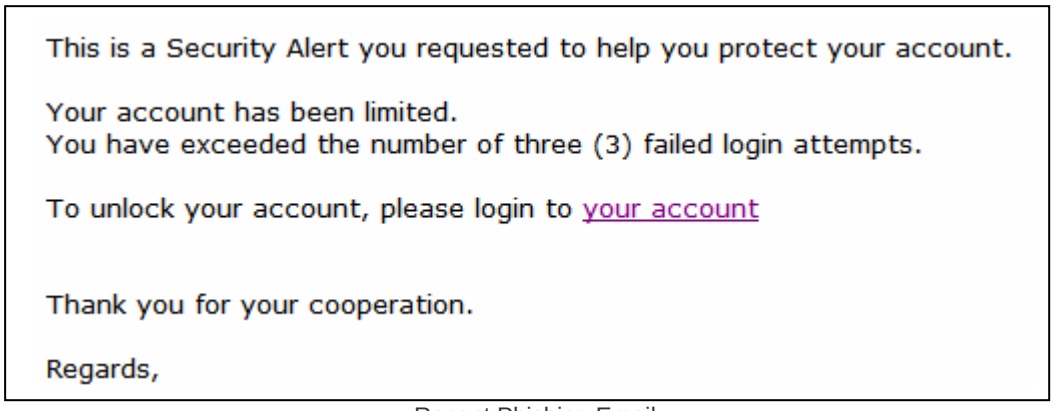
In Session Phishing Attacks

Trusteer Research Paper, December 29, 2008

This security advisory discusses a sophisticated and highly effective phishing attack technique that is carried out while a user is in an active session with a secure banking, brokerage, or other sensitive web application.

Phishing is by far the easiest way to steal login credentials for accessing secure online accounts. For the purposes of this paper, we will use online banking as our sample application. Various utilities allow fraudsters to copy the login page of any bank and set up a fraudulent website within minutes. Once the website is up and running the criminals can start inviting people to “login”, usually using emails pretending to be sent by the targeted bank.

The biggest challenge phishers now face is convincing users to open these malicious email messages and click on the links that lead to the fraudulent websites. The increasing sophistication of spam filtering mechanisms deployed by ISPs and end-users is making it more difficult for these emails to reach their targets. In addition, users are growing more sensitive to security threats and are more suspicious of emails from the “bank”.


This is a Security Alert you requested to help you protect your account.

Your account has been limited.
You have exceeded the number of three (3) failed login attempts.

To unlock your account, please login to your account

Thank you for your cooperation.

Regards,

Recent Phishing Email

Many recent phishing attacks claim to be security warnings, alerting users to suspicious activity in their account or offering a new “security mechanism”. However, this scare tactic is also becoming less effective.

More sophisticated phishing attacks use personal information about the victim to make the email appear more legitimate. These targeted attacks are also known as Spear Phishing. The fraudster collects information on the victim from social networking websites and other resources and uses it to generate a highly creditable email.

Recently the Trusteer research group has been investigating the next generation of phishing attacks with a specific focus on what we call “in-session” attacks.

An in-session phishing attack occurs while the victim is logged onto an online banking application and therefore is much more likely to succeed. A typical attack scenario would occur as follows. A user logs onto their online banking application to perform some tasks. Leaving this browser window open, the user then navigates to other websites. A short time later a popup appears, allegedly from the banking website, which asks the user to retype their username and password because the session has expired, or complete a customer satisfaction survey, or participate in a promotion, etc. Since the user had recently logged onto the banking website, he/she will likely not suspect this popup is fraudulent and thus provide the requested details.

In Session Phishing Attacks

Trusteer Research Paper, December 29, 2008

In order for in-Session phishing attacks to succeed the following conditions are required:

1. A base website must be compromised from which the attack can be launched
2. The malware (injected on the compromised website) must be able to identify which website the victim user is currently logged on to

The first condition is easily achieved, since more than two million legitimate websites are known to be compromised by criminals, and hundreds more are being compromised every day. Each one of them can be used as a base for this attack. Once the website is compromised, the attacker injects code into the website. This code does not change the appearance of the website and does not download malware to the user's PC. Therefore it is very hard to detect. This code is designed to search for online banking websites that visitors are currently logged onto, and present them with a popup that claims to be from the banking website they are logged on to. These pop ups ask for login and personal information.

Identifying websites to which the user is currently logged onto is harder to achieve, but not impossible. For example, in 2006 this blog http://ha.ckers.org/blog/20061108/detecting-states-of-authentication-with-protected-images/ discussed one method that attempts to load images that are only accessible to logged-in users. If the offensive website code is capable of loading the image, this confirms the user is logged on. If it fails, then the user is not logged on. However, most websites do not protect images with login. Instead they are stored on a different server that does not require authentication.

Recently Trusteer CTO Amit Klein and his research group discovered a vulnerability in the JavaScript engine of all leading browsers - Internet Explorer, Firefox, Safari, and Chrome - which allows a website to check whether a user is currently logged onto another website. The source of the vulnerability is a specific JavaScript function. When this function is called it leaves a temporary footprint on the computer and any other website can identify this footprint. Websites that use this function in a certain way are traceable. Many websites, including financial institutions, online retailers, social networking websites, gaming, and gambling websites use this function and can be traced.

To carry out this attack the compromised website needs to maintain a list of websites it wants to check. There is no limit to the number of URLs that a compromised website can check for logged on users. It simply asks the browser a simple question: "is the user currently logged onto this specific website" and the browser will answer "yes" or "no". Once the compromised website identifies a website to which the user is logged on, it can inject a pop up message in the browser pretending to be from the legitimate website and asking for credentials and private information.

To protect themselves from in-session phishing attacks, Trusteer recommends that users:

1. Deploy web browser security tools

2. Always log out of banking and other sensitive online applications and accounts before navigating to other websites

3. Be extremely suspicious of pop ups that appear in a web session if you have not clicked a hyperlink.