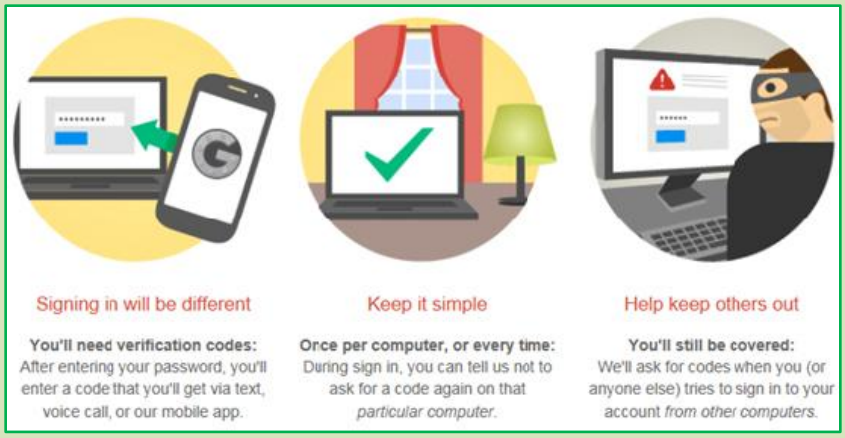
January 10, 2013 Release # 248

-- Begin Transmission --

Phishing 2.0 Targets Business Firms – Final Part

It is advisable to keep our eyes open against phishing. Here are some steps that might be helpful to prevent you from being part of the statistics.



Two-Factor Authentication

Gmail, Facebook, Dropbox, Microsoft, Apple's iCloud gives you the option to use two-factor authentication. In this process you login with a password and a secret code you will receive on your mobile phone so unless the hacker has access to your mobile too, having just your email and your password is not enough to break into your account.

HTTPS Instead of HTTP

HTTPS is a more secure protocol than HTTP as it encrypts your browser and all the information you send or receive. If you are looking to make online payments or transactions, opt for an HTTPS website. Such HTTPS websites are equipped with SSL (secure socket layer) that creates a secure channel for information transition.

Website Reliability

With Phishing, hackers can create a similar website with a normal-looking login page where users enter login details or even credit card details. Therefore, before entering login details users have to check the padlock that appears on the top or bottom part of the webpage. It indicates that the user is communicating with the real website. Many websites have EV (extended validation) SSL certificates that turn address bars into a green bar so users easily recognize authenticity of websites.

Anti Spam Software

With use of anti spam software, phishing attacks can be reduced . Users can control spam mails thus securing himself from phishing.

Hyperlink in Email

Never click hyperlinks received in emails from an unknown or unverified source. Such links may contain malicious codes that may ask you to provide your login details or personal information when you reach the page you are led to after you click the hyperlink.

From the above discussion, users can protect their confidential information from phishing expeditions. SSL is also an important part of online security that protects user against phishing attacks.

-- End of Transmission –

Information Security: It's a Shared Responsibility

REFERENCE(S): www.webroot.com ; http://www.hongkiat.com