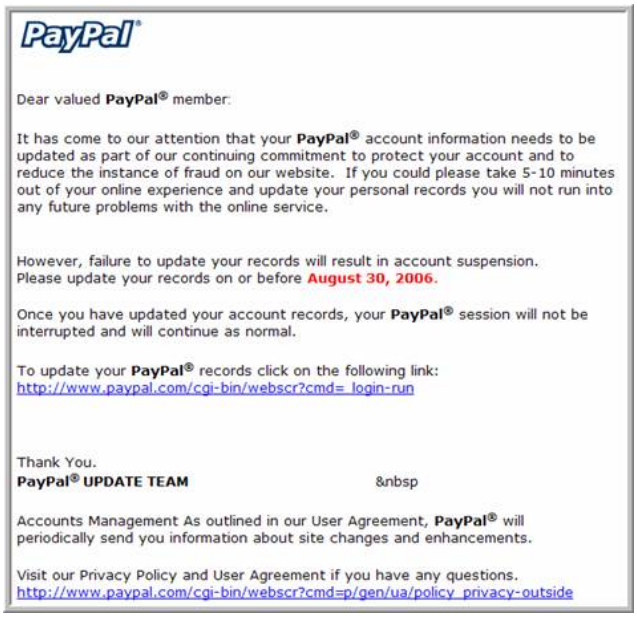
Phishing Scams

Security Update - Best Practices for General User

Phishing refers to the malicious attack method by attackers who imitate legitimate companies in sending emails in order to entice people to share their passwords, credit card or other sensitive personal information. The term comes from the fact that Internet scammers are using increasing sophisticated lures as they "fish" for victims' personal and financial sensitive information.

In order for these Internet scammers to successfully "phish" your personal information, they must first get you to go to visit a website. So, phishing emails will almost always tell you to click on a link that will take you to a website where your personal information will be requested.

The following picture is an example of a phishing email pretending to be from PayPal's customer service representative asking the email recipient to click on the website link to verify user identity:



PayPal

Dear valued **PayPal®** member:

It has come to our attention that your **PayPal®** account information needs to be updated as part of our continuing commitment to protect your account and to reduce the instance of fraud on our website. If you could please take 5-10 minutes out of your online experience and update your personal records you will not run into any future problems with the online service.

However, failure to update your records will result in account suspension. Please update your records on or before **August 30, 2006**.

Once you have updated your account records, your **PayPal®** session will not be interrupted and will continue as normal.

To update your **PayPal®** records click on the following link:
http://www.paypal.com/cgi-bin/webscr?cmd=_login-run

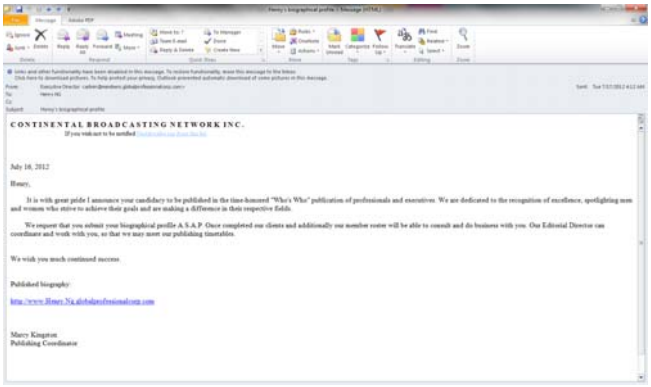
Thank You.
PayPal® UPDATE TEAM

Accounts Management As outlined in our User Agreement, **PayPal®** will periodically send you information about site changes and enhancements.

Visit our Privacy Policy and User Agreement if you have any questions.
http://www.paypal.com/cgi-bin/webscr?cmd=p/gen/ua/policy_privacy-outside

If you click on the link, you will be redirected to a website which looks very similar to the website of the legitimate company. You may be asked to fill in personal information or even keying in the password as part of the verification process. If you do surrender such information, the attacker will immediately capture your personal information.

Another example is the infamous "who's who" phishing scam of which the email recipient receives a congratulation message of being selected as a recognized individual[1]. A link is attached at the end asking the recipient to enter personal information which will be used as published biography.



CONTINENTAL BROADCASTING NETWORK INC.

Clicking on the link will bring to a website which looks like a personalized legitimate professional networking page which requires entering of personal information.

CONTINENTAL BROADCASTING NETWORK
A Who's Who Alliance
Welcome!
Henry Ng.
- Get recognized for your accomplishments!
- Gain credibility in your field!
- Enhance your business and your network!
- Experience career and business growth!
- The possibilities are endless!
Who's Who of Professionals and Executives
Act now to get started with your application process and receive a free listing within the ranks of our alliance. There is never a fee for qualified individuals to be listed.

But after clicking the submit button, the entered information will be sent to a malicious IP address which is probably a collection point by the malicious attackers.

Phishing can also appear in instant messaging programs such as Whatsapp, vChat, Skype type of channels:

Just like the modus operandi of phishing email, the victim will be brought to a legitimate-like web site to surrender personal information if clicking on the links.

Difference between Phishing and SPAM

The term SPAM often appears as another email issue. It is however different from phishing in the sense that SPAM simply refers to unsolicited or undesired bulk electronic messages. But for phishing, the attacker uses social engineering techniques through email or instant messaging to acquire victim's personal information.

Although phishing messages primarily targets to "steal" victim's personal information, some phishing emails will also contain attachments which can contain malicious software. If clicked or activated, spyware such as keylogger, Trojan backdoors or other forms of viruses will be installed on the victim's computer.

Phishing Message Characteristics

The quicker you can recognize a phishing message, the quicker you can ignore and discard to avoid becoming the victim. Phishing messages typically will have the following characteristics:

- Contains deceptive subject lines
- Message content sounds interesting
- Appears to come from legitimate organization (e.g. banks, Government, online merchants)
- Email includes hyperlink(s) which appears to point to legitimate organization's web-site
- Include threats "if you do not fill form, we will block your account"
- Contains forms requesting to fill out personal information
- Contains attachments like PDF's or Word documents that will download and install malware to computer if activated

In order to entice as many victims as possible to view the content and click on the links, very often the phishing messages will pretend to be from large and well recognizable companies. The following are some of the companies that were often fraudulently represented in phishing emails[2].

	Top 10 Identified Targets	Valid Phishes
1	PayPal	10,497
2	eBay, Inc.	692
3	Poste Italiane	456
4	AOL	441
5	Apple	430
6	Cielo	253
7	Bradesco	233
8	Internal Revenue Service	216
9	Itau	211
10	JPMorgan Chase and Co.	195

In Hong Kong, Hong Kong Monetary Authority has issued 36 public alerts of detecting fraudulent bank web sites and phishing emails in 2014 alone. Overseas banks and locally present banks including HSBC, Bank of China and Standard Chartered Bank were among the targets of phishing scams[3]. So users should pay extreme cautions if receiving messages of such nature.

Stay Alert of Spear Phishing

Spear phishing is a sophisticated attack attempt directed to a specific individual or company. Typically, attackers will perform extensive reconnaissance about the targeted individual. A customized email will then be sent to the individual, with content reflecting knowledge about the target individual's work activities, colleagues, friends, or family. The message can include a link or attachment leading to infection of the target's computer, often with custom malware. TrendMicro Labs reported that 70% of monitored spear phishing messages contain malicious attachments with the most commonly used and shared file types of companies such as .XLS, .PDF, .DOC.[4]

A number of high profile advanced persistent threat attacks, (e.g. Anthem hack of personnel data[5]) started off by sending spear phishing emails to targeted individuals. Once infecting the individuals with malware, the attackers will then launch sophisticated hacking to retrieve sensitive corporate information.[6]

How to Prevent Phishing

As a general rule of thumb to avoid being a phishing victim, be sceptical when reading messages about submitting personal information. There are other recommendations from Hong Kong InfoSec[7] and APWG[8] web sites which are summarized as follow:

Be suspicious of emails with urgent request for personal information

Phishers take advantage of upsetting or exciting (but false) messages to get people to hand over their information such as usernames, passwords, credit card numbers, date of birth and other personal information.

Don't trust links in an email

Pay attention to the website you are being directed to and hover over the web link. An email that appears to be from PayPal could direct you to a fraudulent website such as

http://www.2paypal.com
or
http://www.gotyouscammed.com/paypal/login.htm

Never give out personal information upon email request

Legitimate companies will hardly request their customers to give out personal information over just an email request. Nor will these companies request you to fill in personal information over a web form. If in doubt, call the company to verify.

Inspect the web address carefully

The web address of some phishing websites will look almost the same as the legitimate companies in order to deceive heedless users. Double check the web address or even type the address in the browser instead of clicking on the link.

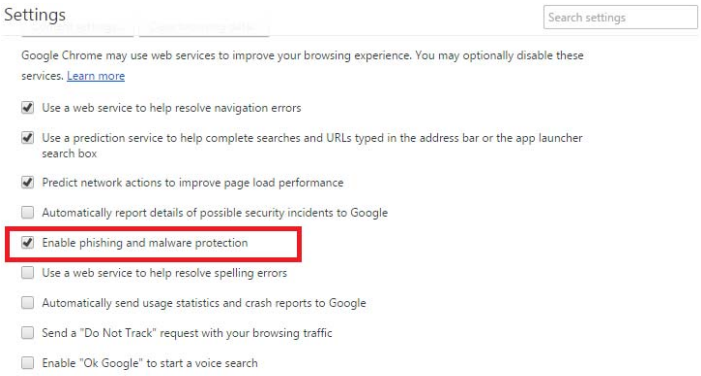
Don't open unexpected email attachments or instant messaging download links

This is the most common way for attackers to spread computer viruses or install malicious software. Be suspicious if you are not expecting an email which comes with an attachment. Use updated anti-malware programs to scan the attachments before opening. These days, computer viruses can be embedded in all kinds of attachments including Word, Excel, PDF and executive files.

Enable anti-phishing features of web browser

Some web browsers have built in anti-phishing features. For instance, Internet Explorer comes with SmartScreen filter. For Safari, Firefox and Chrome, anti-phishing features can be enabled under security settings.

The following diagram illustrates the security configuration settings of Chrome browser to enable anti-phishing feature:



There are also external plugins and anti-virus software which can be installed to further enable anti-phishing feature. These can help reduce the chance of mistakenly visiting a phishing web site.

Phishing on Social Media

Because of the popularity of social media, phishing scams are moving from traditional email based to social media platform. Fake web links, fraudulent web pages and forms requesting for personal information are posted on some social media sites with the malicious intention of capturing user's personal information.

In addition to the phishing email precautions, users can adopt the following best practices to avoid phishing on social media platform:

- Don't click on links in social media asking to claim amazing prize (especially pop ups)
- There are many fake Facebook pages. If a Facebook page asks you to login after you already did, check the URL. Even if the URL includes the name "facebook", it does not mean it legit (https > http)
- Don't respond to emails asking for personal information, Facebook and social medias sites would never ask for such information over email
- Never give your personal information to emails claiming to be from certain social media sites
- Do not accept friends or connections hastily you don't know as three friends or more can help you change your password
- Email phish@fb.com or the equivalent for other social media sites, if you should report a phishing attack

Phishing on Mobile Devices

Besides social media platform, there is also a rising trend for phishing messages to target mobile devices. They can be spread via install messaging platform with messages containing malicious website links. Because of the small form factor of mobile screens, users typically will not check the authenticity of the web address when clicking on the link.

Also, shorten URL services are often used on mobile devices (e.g. bit.ly, goo.gl, etc.) to convert long URLs into shorten ones. Phishers can easily hide malicious links using these shortened URL web addresses. Users should be aware of the risks of phishing on mobile devices[9].

What should do when becoming a Phishing Victim

If you have unfortunately fall prey to a phishing attack, the following immediate measures are strongly recommended:

- Change passwords, PINs and security questions for the affected online services
- Run your computer with anti-malware software to verify installation of any malicious programs
- Check your credit card or online bank account and report to the bank for suspected fraud cases
- Inform your friends if the phishing message was forwarded onto them
- Report the case to the University IT security help desk or police for investigation

References

1. “Who's Who scam - Wikipedia” WEB Feb 17, 2015
2. “Phishtank” May 2014 WEB Feb 17, 2015
3. "Fraudulent Bank Websites and Phishing E-mails – Hong Kong Monetary Authority” WEB Feb 17, 2015
4. “Trend Micro Incorporated Research Paper 2012” PDF Feb 17, 2015
5. “Anthem hack: Personal data stolen sells for 10X price of stolen credit card numbers” Feb 6, 2015 WEB Feb 17, 2015
6. “New spear phishing campaign targets universities, government contractors and security companies” Jun 13, 2012 WEB Feb 17, 2015
7. “Protecting Against Phishing Attacks – InfoSec” WEB Feb 17, 2015
8. “How to Avoid Phishing Scams – APWG” WEB Feb 17, 2015
9. “Beware of phishing website when using mobile device” Jan 16, 2013 WEB Feb 17, 2015
10. “Wikimedia Commons” WEB Feb 18, 2015

Copyright Statement