REMINDER: Emailed to a group account. Do NOT reply using email group account.
For comments or inquiries email infosec@pjlhuillier.com.

May 3, 2013 Release # 213

-- Begin Transmission --

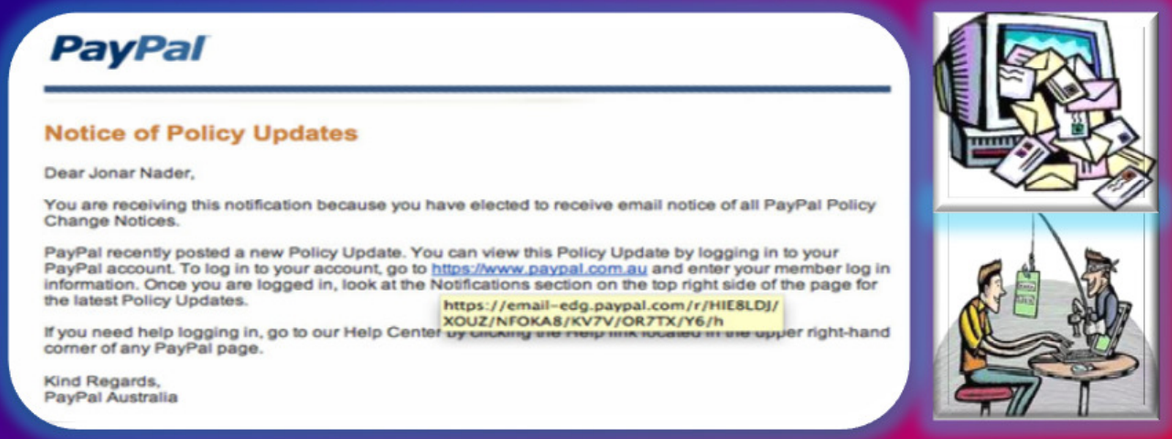
Top 10 Social Engineering Tactics – Part 3

Top 10 Social Engineering Tactics – Part 3

7. Catch Me a Phish

A phishing attack occurs when a social engineer sends an email to a person who appears to come from a legitimate site, such as PayPal or a banking site, asking someone to visit a website and input sensitive information (bank account user name and password). The website appears to be the real website, but is a duplicate site created by the attacker.

Here is an example from an actual phishing email where the attacker impersonated an employee of PayPal:



PayPal

Notice of Policy Updates

Dear Jonar Nader,

You are receiving this notification because you have elected to receive email notice of all PayPal Policy Change Notices.

PayPal recently posted a new Policy Update. You can view this Policy Update by logging in to your PayPal account. To log in to your account, go to https://www.paypal.com.au and enter your member log in information. Once you are logged in, look at the Notifications section on the top right side of the page for the latest Policy Updates.

https://email-edg.paypal.com/r/HIE8LDJ/XOUZ/NFOKA8/KV7V/OR7TX/Y6/h

If you need help logging in, go to our Help Center by clicking the Help link located in the upper right-hand corner of any PayPal page.

Kind Regards,
PayPal Australia

This e-mail provided a link to a fake website for the e-mail recipient to access and input credit card information.

If a social engineer is able to glean information specific to a person, such as a name or address, the engineer can take the phishing scam a step further and include this information in the email to make it appear more legitimate. This type of targeted attack is called a **spear phishing attack**.

6. A Whale of an Attack

Another variation of phishing attacks is a **whaling attack**. Here, the social engineer targets high-profile executives because their information is easily accessible on the Internet. For example, a company may publish biographies of its executive officers on the corporate website. The published information may be used by a social engineer in planning for an attack against them.

For example, if the biography tells how a chief financial officer graduated from Duke University in 1979 and enjoys playing golf (yes, some executives actually put their hobbies in their bios), a social engineer may send an email to that corporate officer as if from the university alumni chapter asking him to come to a special alumni golf tournament for graduates. The executive will be likely to believe that it is authentic. The email may go on to ask the person to access a website to enter credit card information to reserve a spot in the tournament.

Because information about corporate officers and other high-profile targets are readily available over the internet , whaling is becoming increasingly popular which makes it so easy for social engineers to convince them and become victims.

…to be continued

-- End of Transmission --

Information Security: It's a Shared Responsibility
REFERENCE(S): http://www.informit.com/

INTERNAL USE ONLY: For circulation within the PJ Lhuillier Group of Companies only.