

PROTECTING YOURSELF AGAINST PHISHING SCHEMES

Phishing

This is not a misspelling, but an Internet/email scam to steal your personal information. The phisher's goal is to obtain passwords or personal information that can be exploited to his or her benefit.

Beware of any email asking you supply information by clicking on a link.

Steps to Protection

- Never use email links to access websites where you must login using a username and password. If you engage in online financial transactions, always type the web address in yourself and verify that you spelled it correctly before pressing enter or clicking Go.

Reputable companies do not ask you to confirm passwords, account numbers, or other personal information through email. Beware of these fear tactics, prompting you to immediate action. If in doubt, contact your financial institution by phone to determine if there is a problem with your account and how to resolve it.

- If you suspect a phishing email, you should forward that email as an attachment to that financial institution for their investigation, with hopes that the perpetrators of the scam will get caught. Just because the link in the email looks like your bank's web address does not mean that it links to your bank's website.
- Call or visit your financial institution and find out what their policies for contacting you are, how they handle potential fraud and verifying your identity. For example Chase bank and PayPal both provide information online to protect yourself from identity theft.
- Also beware of quick money schemes, schemes of large sums of money overseas to place into your bank account, and deals that are too good to be true. Again, they are after your bank account information. They want to take, not give.

PROTECTING YOURSELF AGAINST PHISHING SCHEMES

There is no way to prevent receiving these emails. Financial institutions and PayPal do send legitimate emails, so you need to be informed on how to tell the difference between legitimate emails and phishing scams. Remember perpetrators of these scams are relying on two human emotions: fear and greed. Instead, be informed and use common sense.

For more information on spoofing, phishing, and identity theft, check out the following websites:

<http://en.wikipedia.org/wiki/Spoof>

http://www.webopedia.com/TERM/E/e_mail_spoofing.html

<http://pages.ebay.com/education/spoofutorial/>

<http://www.paypal.com/cgi-bin/webscr?cmd=xpt/general/SecuritySpoof-outside>

<http://www.ftc.gov/bcp/edu/microsites/idtheft/>

<http://onguardonline.gov/index.html>