March 4, 2016

**Alert - Phishing Emails**

**What is Phishing?**
Phishing is an attempt to deceive you into thinking a legitimate organization is requesting information from you. These requests for information may look innocent at first glance or may seem to come from a legitimate source, but they do not. These scams request you reply to an email or follow a link to a web site.

Email phishing attempts frequently give clear indications that the request is not legitimate. Links to web sites (sent to you through email) often take you to web pages that look very similar to the legitimate service the email is faking. Banks, eBay, and PayPal are common targets. Also, more sophisticated phishing attempts are sometimes targeted against specific “high-value” groups of individuals and are called “Spear Phishing,” because of their more directed focus.

**What does a Phishing email look like?**
Phishing emails often attempt to use emotional triggers to get you to react quickly without thinking through whether you should respond, such as dire language about time limits, loss of service, or financial penalties. They often have grammar or spelling errors, and/or phrasing that is not normally used.

An example of a Phishing attempt would be an email with a generic greeting, warning of a change in one of your accounts, requiring you to verify your account information. These emails typically include directions to reply with private information, or provide a link to a web site to verify your account by providing personal information such as name, address, bank account numbers, Social Security numbers, or other sensitive personal information.

**Will DPH send legitimate emails that look like Phishing scams?**
NO. There will be times when legitimate messages must be sent to inform our email users of various issues. These may include password expiration notices or informational emails, such as this one. However, it is very important to remember that the DPH IT department will never ask for your password, nor should you ever give it out.

**Why can’t DPH stop these emails?**
DPH actually stops thousands of Phishing attempts, spam emails, and virus infected emails daily, but the methods scammers use change very quickly. Also, due to the great variety of uses for DPH email, we must be careful not to implement filtering which may block legitimate emails.

**How can I avoid Phishing scams?**

- Never send passwords, bank account numbers, or other private information in an email.
- Avoid clicking links in emails, especially any that requests private information.
- Be wary of any unexpected email attachments or links, even from people you know.
• Look for ‘https://’ and a lock icon in the address bar before entering any private information.
• Have an updated anti-virus program installed that can scan email.

If you are ever in doubt about the legitimacy of an email, please call the DPH Help Desk at 415-759-3577 or email them at: dph.helpdesk@sfdph.org

Thank you,
George Powers, CISM, CISSP
Acting Director, IT Systems, Networks, and Security Operations
Department of Public Health
City and County of San Francisco