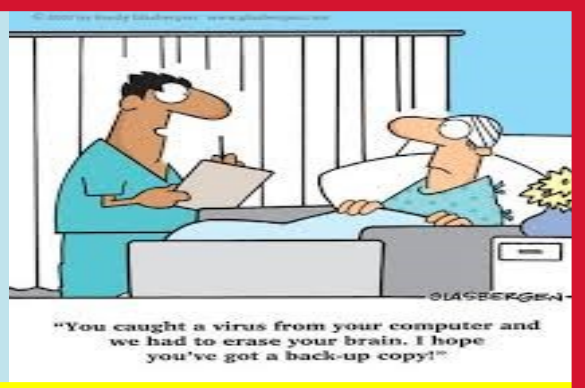
# U.S Public Health Service

# Nursing Tip of the Month

# May 2017

# Cyber Security




## Helpful Information How To Protect Yourself from Cyber Attacks

**The following preventative strategies are intended to help our public and private partners proactively look for emails attempting to deceive users into "clicking the link" or opening attachments to seemingly real websites:**

- **Never click on links in emails**. If you do think the email is legitimate, whether from a third party retailer or primary retailer, go to the site and log on directly. Whatever notification or service offering was referenced in the email, if valid, will be available via regular log on.
- **Never open the attachments**. Typically, retailers will not send emails with attachments. If there is any doubt, contact the retailer directly and ask whether the email with the attachment was sent from them.

- **Do not give out personal information** over the phone or in an email unless completely sure. Social engineering is a process of deceiving individuals into providing personal information to seemingly trusted agents who turn out to be malicious actors. If contacted over the phone by someone claiming to be a retailer or collection agency, do not give out your personal information. Ask them to provide you their name and a call-back number. Just because they may have some of your information does not mean they are legitimate!
- https://www.dhs.gov/how-do-i/protect-myself-cyber-attacks for a complete head-to-toe cyber checkup – and keep your identity safe!

**Phishing or Social engineering** is a process of deceiving individuals into providing personal information to seemingly trusted agents who turn out to be malicious actors. If contacted over the phone by someone claiming to be a retailer or collection agency, do not give out your personal information. Ask them to provide you their name and a call-back number.

**Phishing attacks** may also appear to come from other types of organizations, such as charities. Attackers often take advantage of current events and certain times of the year, such as:

- natural disasters (e.g., Hurricane Katrina, Indonesian tsunami)
- epidemics and health scares (e.g., H1N1)
- economic concerns (e.g., IRS scams)
- major political elections
- holidays

### Practical tips to protect yourself from cyberattacks:

• Set secure passwords and don't share them with anyone. Avoid using common words, phrases, or personal information and update regularly. Don't use passwords that are based on personal information, it makes it easier for an attacker to guess or "crack" them.

• Keep your operating system, browser, anti-virus and other critical software up to date. Security updates and patches are available for free from major companies.

• Verify the authenticity of requests from companies or individuals by contacting them directly. If you are asked to provide personal information via email, you can independently contact the company directly to verify this request.

• Pay close attention to website URLs. Pay attention to the URLs of websites you visit. Malicious websites sometimes use a variation in common spelling or a different domain (for example, .com instead of .net) to deceive unsuspecting computer users.

• For e-mail, turn off the option to automatically download attachments.

Available resources:

https://www.consumer.ftc.gov/scam-alerts

Advice about common security issues for non-technical computer users

Information about current security issues, vulnerabilities, and exploits

Weekly Summary of New Vulnerabilities

OnGuardOnline.gov

**Points of contact: CAPT Casey Hadsall, CDR Jonathan Paulsel, & LCDR Anastasia Hansen for the Mentoring Workgroup, N-PAC Career Development Subcommittee.**

**PHS-NURSE LIST SERV**

**TO REQUEST A MENTOR**