Anthelio Healthcare Solutions
Global Information Security Group
Security Awareness Bulletin - Vol. 05

anthelio®
A higher aim. A newer standard.

E-mail and Web Security

Spyware, ransom-ware, bots, payloads, phishing. Once buzz words, these have become all too common. Thanks to the media and its focus on security news stories, it has heightened the awareness. However, even with a raised awareness, individuals still regularly fall victim to malicious campaigns, with the message content becoming incredibly convincing, tricking users to click or download items carrying malware. Research indicates that e-mails and malicious websites are among the easiest sources for exploitation, and the attack methods continues to be effective and successful, causing significant disruptions to business.

In general terms, standard e-mail is similar to a physical postcard, where the message content, recipient name and address are visible to everyone to be read. Every letter handler and post office hub along the way can potentially read the message content while it is en-route to its destination.

Likewise, e-mail messages also cross the network and travel through computers and hubs along the Internet before being delivered to the intended recipient. A malicious person controlling a portion of the network could intercept e-mails, and read, alter, or copy the message content undetected by the sender or recipient.

Just like postcards, standard e-mails lack a secure envelope to keep the message content private while it's being sent across the Internet. While technology exists to limit the spam e-mail(s) entering the organization, some still evade and reach the user's inbox. It is important that everyone be vigilant, and never respond to e-mails that ask for passwords, confidential, or private information, without verifying and validating the legitimacy. Here are some ways to safeguard and protect the **content** and the **communication:**

E-mail security

- Do not send confidential information using standard e-mail; instead use Secure e-mail.
- Do not open suspicious e-mail attachment(s) especially from unknown sources. If in doubt, copy the e-mail and attach it to a new e-mail addressed to report.spam@antheliohealth.com, and then delete it.
- Pay very close attention to the sender of the e-mail and who you are replying to. Before hitting SEND, verify the TO: address. If it looks suspicious – do not Send; instead report it to Service Desk.
- Do not click links in an e-mail, instead type the link-address in a browser.
- Learn to identify SPAM e-mails.

Reference: https://home.phns.com/IT_services_org/infosec_org/PublicLibrary/Public%20Documents/Awareness/STH-Poster-DontGetHooked-Email.jpg

Web security

- Limit your web browsing to well-known, trusted and secure websites that use encryption (https). If a website asks for private or confidential information and doesn't use HTTPS– immediately exit.
- Do not access financial websites or share private information when using public Wi-Fi. Avoid using Company devices on a public Wi-Fi. Should the need arise connect to VPN.
- Ensure Anti-Virus software is current, up-to-date and running at all times.
- Do not install web browser plugins, and don't click on pop-ups or ads. If there is legitimate need for these services, contact the Anthelio National Service Desk.
- Be cautious when accessing websites from public computers. Remove the browser cache, logoff from website(s), close all browser activity, before exiting.