CYBER SECURITY AWARENESS MONTH TIPS OF THE DAY

WEEK 2

From the Break Room to the Board Room - Cyber Security at Work

Businesses face significant financial loss when a cyber attack occurs. Cybercriminals often rely on human error – from employees failing to install software patches to clicking on malicious links – to gain access to systems. From the top leadership to the newest employee, cybersecurity requires the vigilance of every employee to keep data, customers, and capital safe and secure.

Organizations of any size – including healthcare providers, colleges and universities, government agencies and nonprofits – can fall victim to cybercrime, which could result in stolen customer data or intellectual property, and business disruptions. For 2017, the top threats facing businesses are ransomware and extortion, Internet of Things (IoT) security threats and insider threats. As these cybersecurity threats continue to grow in size and magnitude, companies large and small need to develop a cyber action plan and be aware of the evolving threat landscape.

- 65% of professionals identified phishing and social engineering as the biggest security threat to their organization. All it takes is one person clicking a fake email about banking or spyware to give a hacker direct access to all the data on their device and a direct path to your network.

Monday, Oct. 9, 2017

How to Spot a Phishy Email

Phishing attacks use email or malicious websites to infect your machine with malware and viruses in order to collect personal and financial information. Cybercriminals attempt to lure users to click on a link or open an attachment that infects their computer with viruses or malware, creating vulnerability to attacks. Phishing emails may appear to come from a real financial institution, e-commerce site, government agency, or any other service, business, or individual. The email may also request personal information like account numbers, passwords, or Social Security numbers. When users respond with the information or click on a link, attackers use it to access their accounts.

Click the link to find out the red flags that could tip you off to a potentially phishy email: https://www.vbgov.com/residents/public-safety/practice-safe-cyber/Documents/How%20to%20Spot%20a%20Phishy%20Email%20[Infographic].pdf

Wednesday, Oct. 11, 2017

How savvy are you about being safe online at work?

Did you know that employees are the weakest link when it comes to cyber security for businesses? Take the Hyphenet Employee Security Quiz and find out how much you know about workplace cyber security.

Friday, Oct. 13, 2017

If you experience anything suspicious involving your computer at work, report it to your IT department or designated Information security personnel at your organization. Suspicious activity could be any of the following: system failure or disruption, unauthorized access requests, suspicious emails from unknown sources or, unauthorized changes or additions to your system's hardware, software or firmware without your IT department's knowledge. Any of these activities should be reported to your company's IT department immediately to protect the security of your organization's computer systems.