2019 Cybersecurity Webinar Series

10.25.18

In honor of National Cybersecurity Awareness Month (NCSAM), BPM is excited to announce our 2019 Cybersecurity webinar series. Every day businesses and individuals are at risk for online fraud and threats, however you can protect yourself and your business by learning cybersecurity fundamentals and proactively developing a cybersecurity mentality. Be on the lookout for our upcoming webinars featuring topics such as identifying scam and phishing emails, GDPR, web application vulnerabilities and cleansing habits, and more.

Top Five Cybersecurity Tips for 2019

1. Always Be on the Lookout for Scams
When it comes to cybersecurity, don't be fooled, they are out to get you. By remaining vigilant about every phone call, email, and in-person interaction you have (especially ones you don't initiate), you will be much more successful spotting social engineered attacks.

2. Use Strong Passwords
The only strong password is a long password that has been securely stored. Consider using passphrases; they are strong, easy to remember, and surprisingly easy to type. Also, remember to encrypt the storage of your passphrases. Even if you're just using a spreadsheet to store your passphrases, put a password on it.

3. Secure Your Browser
Keep your browser patched/updated and always "enable" privacy settings. Even though it may degrade your browsing experience, consider privacy/security browser add-ins like:

- No-Script: to prohibit a staggering number of scripts that attempt to run in the background
- Privacy Badger: to limit advertisement, cookie information harvesting, and tracking tools
- Foxy Proxy: to hide your point of origin

4. Don't Use Email for Sensitive Conversations & Attachments
If you must use email for sensitive conversations, consider strong encryption tools like PGP or Zixmail. Otherwise, use encrypted messaging tools like WhatsApp or Telegram.

5. Verify URLs Before Clicking
Hover over links before clicking and, if the link revealed by hovering doesn't match, DO NOT CLICK! Instead, pay extra attention to the word immediately preceding the .com. .org, etc. because is the domain you're actually visiting. If the final word before the .com is not exactly, letter-for-letter where you intend to go, don't go there.

By David Trepp, Information Security Assessment Services Leader