

Cyber Awareness Month – A 2022 Perspective

By Thomas J. DeMayo, Principal, Cybersecurity and Privacy Advisory

October has been designated as Cybersecurity Awareness Month; very appropriately, it's also the month of ghosts and goblins. In recognition of the month's cyber awareness objective, let's all step back and take into consideration how extensively the threat has evolved over the past few years. It is now, more than ever, a part of our everyday lives and we must avoid the cyber tricks so we may benefit from the treats.

Scary Backdrop

In 2020, the pandemic uprooted our normal work routine and ushered in the era of remote and hybrid work. The cyber criminals were quick to respond and exploit the technical and emotional distress that this monumental shift brought with it.

In 2021, we witnessed the cyber criminals target the supply chain reminding us that we truly are only as strong as our weakest link. In a cloud and mobile world, our connections and dependencies cannot be overlooked or forgotten.

In 2022, Russia attacked Ukraine, flexing not only the country's physical might and nuclear capabilities, but also unveiling its cybersecurity warfare strength. Ultimately, this demonstrated that in a globally connected world, borders fade away and the attackers lurk in the shadows of the connectivity we depend on.

Some Tips

We prepare for the future by understanding and respecting our past. Our past has taught us that cybersecurity threats will remain a persistent evil that we must identify and respect, against which we must also defend our families, friends and businesses. In this month dedicated to cyber awareness, we offer the following considerations:

- **Be aware.** Never stop learning and understanding what the cyber threat is and how you should defend against it.
- **Invest in yourself and your people.** Cyber threats target not only technical weaknesses, but emotional weaknesses as well. Cybersecurity is equally, if not more, about people and behaviors as it is about technical solutions.
- **Pause, Inspect and Think (PIT)** before clicking any links, opening any attachments or visiting websites. Introduce that mantra into your daily life and workplace. This applies across all potential channels: e-mail, social media, text messaging, messaging apps, etc.
- **Make sure your systems are patched** consistently and frequently with vendor-supplied security updates. Updates count. The U.S. Cybersecurity & Infrastructure Security Agency (CISA) maintains a listing of vulnerabilities that are actively exploited [\[here\]](#). Review this listing with your IT team and make these a priority.
- **Embrace multi-factor authentication (MFA).** Passwords alone are not effective. If you have not yet deployed MFA, now is the time to do so.
- **Implement GEO IP Address restrictions.** If your business does not have any reason to communicate with certain countries, block those countries.
- **Monitor your systems and user activity.** You can't respond if you don't know you have an issue.

- **Ready your incident response plans or create one.** Incidents will occur and, when they do occur, your stakeholders will be watching how you respond.
- **Know your limitations and when to seek assistance.** Strategically utilizing third parties that have expertise in cybersecurity and privacy to help identify and manage your risk can bridge the resource and knowledge gap you have internally.
- **Test.** Penetration testing to simulate a cyber threat actor will help identify technical weaknesses and visibility limitations in your monitoring and response processes.

Stronger Together

We are all in this together and, as a Firm, we are here to help play our part. Cybersecurity can seem daunting and at times makes you feel helpless; however, with the proper attitude, resources and risk-aligned practices, it can be overcome and managed. Let us help to demonstrate not just Know Greater Value, but also, Know Greater Cybersecurity.

Contact Us

Thomas J. DeMayo, CISSP, CISA, CIPP/US, CRISC, CEH, CHFI, CCFE
Principal
Cybersecurity and Privacy Advisory
tdemayo@pkfod.com | 646.449.6353

Nick DeLena, CISSP, CISA, CRISC, CDPSE
Partner
Cybersecurity and Privacy Advisory
ndelena@pkfod.com | 781.937.519

Our Firm provides the information in this e-newsletter for general guidance only and it does not constitute the provision of legal advice, tax advice, accounting services, or professional consulting of any kind.