proofpoint.

SOLUTION BRIEF

Five Considerations for Security Awareness Training During Emergency Situations

In times of crisis, cybersecurity best practices can be more critical than ever

When infosec and IT resources are constrained due to a local, regional, national, or global emergency, curtailing security awareness training initiatives can offer a quick way to free up time and staff members for business-critical continuity exercises. But that approach can also leave your end users (and your organization) more vulnerable.

Here are five important things to think about before pulling the plug on your program during a prolonged crisis:

1. **Threat actors and cybercriminals are opportunistic** — Fear, curiosity, and uncertainty run high among individuals during a time of crisis (like a widespread natural disaster or pandemic). We know that fraudsters take all opportunities to exploit these emotions among end users. It's critical that employees be made aware of the lengths attackers will go to, and the ways threat actors will attempt to fool them. (You can find examples of real-world messages and lures in our ThreatSim® Phishing Simulations library. As well, our Attack Spotlight campaigns highlight widespread attack trends and offer advice and training to combat these threats.)
2. **Users may end up in unfamiliar working environments** — Crisis stiuations might force employees to shift to temporary worksites or other remote working situations. Users likely need to consider an expanded set of cybersecurity best practices in these settings. Don't make assumptions about the security of remote networks, and don't expect employees to figure things out on their own.
3. **People often seek certainty in times of uncertainty** — This point builds on the prior two. The average person wants to feel as empowered and centered as possible during times of uncertainty. If you take your voice out of the mix, you will give threat actors more power. It's critical that, from a cybersecurity perspective, a trusted authority remain the voice of reason and provide guidance on what to do to stay more secure — and how to do it.
4. **Your coworkers may be willing and able to assist you** — During times of crisis, many individuals are willing to stretch beyond regular skillsets and/or responsibilities in order to support the "greater good." Don't discount the role that direct managers, HR, legal/compliance, and even marketing teams may be willing to take on in order to communicate important messages related to cybersecurity best practices. Others may be able to keep a program running while infosec and IT resources are tied up on other things.

5. **Doing something is better than doing nothing** — There could be situations in which you have to temporarily suspend formal phishing and training exercises because of an ongoing emergency environment. But we encourage you to go into "awareness mode" rather than completely stopping a security awareness training program. You can do this by focusing on information-sharing tools, like the campaigns, awareness videos, articles, infographics, and newsletters available in our Security Awareness Materials (SAM) Portal. These materials are purpose-written for end-user audiences; they can help you introduce and reinforce key cybersecurity initiatives, and keep security behaviors top-of-mind for employees. During times of crisis, attention to personal behaviors and actions can be more important than ever. You should not leave those behaviors to chance.

LEARN MORE

For more information, visit **proofpoint.com**.