CYBERSECURITY AWARENESS DURING A CRISIS

coretelligent
THE POWER OF IT™

CYBERSECURITY AWARENESS DURING A CRISIS

With any headline-grabbing crisis, there is the inevitable and unfortunate side-effect of scammers and cyber-criminals looking to exploit and profit via people's fear or uncertainly surrounding the situation.

In the past week, where the news and social media headlines have been dominated by the COVID-19 pandemic, companies are rushing to find ways to securely scale and support employees working from home.

If you received an email notification from the Centers for Disease Control and Prevention or the World Health Organization about the Corona virus outbreak, would you read it? Perhaps even click on a link? Or perhaps a plea from your local town, school, or organization soliciting donations for people/areas impacted?

...Scammers and cyber-criminals are counting on it.

It is critical for employees to know how to spot the warning signs of a phishing email, and the impact it can have to them and the organization at large.

Common phishing email topics or scenarios may include:

- Request for donations (monetary, supplies, etc.)
- Vendor Payments or Order Requests
- Wire Fraud (always a popular scam)
- State or Town Security/Health Updates
- Medical Scams – provide your Social Security #, etc.
- Personal Information Updates or Validation Requests
- Scams focused around WFH technologies (validate your password, test your VPN, etc.)

COMMON STEPS THAT USERS SHOULD TAKE TO REMAIN SAFE DIGITALLY

TRUST NO ONE / ZERO TRUST

Sadly, the modern Internet is a dangerous place, and we all must adopt a "Zero Trust" policy to help keep us safe while operating in an always online/connected world.

Ask yourself – is this a contact/organization that you have communicated with in the past, or is this a brand-new communication? If this is a net-new contact to you, with a very complicated or aggressive request or demand, this should also give you pause.

While the general formatting, grammar, and sophistication of phishing messages has improved dramatically, you can still sometimes spot irregularities.

BE AWARE

Always know what you are downloading and where you are downloading it from.

Download applications directly from the developer/seller and avoid 3rd party download sites whenever possible.

Avoid clicking on popup windows or inadvertently entering your password into the incorrect window or application.

PASSWORD MANAGEMENT / MULTI-FACTOR AUTHENTICATION

Always safeguard your passwords and avoid entering them into strange websites or pop-up windows. Verify that the application or website asking for the password is a site that SHOULD have access to your username and/or password.

Ensure you are leveraging two-factor/multi-factor authentication for sensitive sites/logins wherever possible.

Avoid re-using the same password across multiple sites or applications. At this point, it is not IF, but WHEN a website or service may likely have a data breach, which means the likelihood of your email and/or password used on that site may be compromised.

Consider using a password manager to securely track, manage, and rotate your sensitive passwords (both personal and professional).

LINKS & ATTACHMENTS

When in doubt, do NOT click on any odd or suspicious links in an email. The same applies for email attachments from unknown or new senders. Never save or open them on your machine if you are unsure of their validity or origin.

To be safe, forward the email to your IT department or IT consultancy to review/validate on your behalf.

Alternatively, if you hover your mouse cursor over a link in the email, you will see the underling address that it redirects to. If the URL doesn't match the sender/organization, this is another sign that the message could be spam or a phishing attempt.

TRAINING

As a business, ensure that you are regularly testing & training your users for cybersecurity awareness to ensure they are adequately informed and prepared to navigate the ever-evolving threat landscape.

This can be accomplished through a variety of methods and tools, including simulating phishing emails and measuring who clicks into them (engaging in risky behavior), self-guided training videos via online platforms, or live "lunch and learn" cyber training.

While no organization can claim 100% immunity against cyber-threats, and no user can ever be 100% trained/safe against phishing threats, by following these strategies you can help reduce your risk of becoming a victim of these scams.

To learn how Coretelligent can help you manage cyber threats and reduce costs, visit www.coretelligent.com or call 855.841.5888

ABOUT CORETELLIGENT

Coretelligent is the IT support and private cloud service provider of choice for small and mid-sized businesses nationwide. Led by world-class technology experts, Coretelligent offers four best-in-class services covering the full range of technology needs: 360 Support, CoreCloud, CoreBDR, and CoreArmor. Top-tier organizations in the financial services, life sciences, technology, legal, and professional services sectors rely on Coretelligent to help maximize their technology return on investment. Founded in 2006, the company has offices in Massachusetts, Maine, New York, Pennsylvania, Stamford, Georgia, and California.