PROJECT CYBERSAFE™

BULLETIN

May 2025

Important Tools to Have in Your Cybersecurity Tool Belt

Phishing awareness continues to be the foundation of the human firewall for protecting your business from a cybersecurity incident.

Domain impersonation is on the rise and AI created phishing emails are starting to outperform human phishing attempts. These emails are looking more realistic, with less grammatical errors than human created threat emails. Being able to recognize phishing emails continues to remain a challenge.

This KnowBe4 article highlights the increase of legitimate domains being impersonated by cybercriminals in phishing attacks.

Using these tips below will reduce your chances of engaging with an email that could put your company at risk.

Were you expecting it?

Was the invoice or request for payment expected from the sender of the email? If not, Delete and Move On!

Hover over the link and Think Before You Click:

Always hover over the hyperlink to see where the URL is directing you to. This becomes difficult when interacting with an email on a mobile device. Always engage with suspicious emails on your computer where you can reduce your chance of an accidental click or download.

Go to the source.

You can always go to the source of the request. Whether the email purports to be from Docusign, Dropbox, or your company's messaging app, you can always log in to the webpage of the service or application to verify its authenticity. Similarly at home, any text messages that claim to be from your bank can be confirmed by logging into your bank website or app instead of trusting the text message link.

Call the sender.

Do not be afraid to reach out directly to the sender when an email does not appear legitimate. Whether it is the lack of an email signature, unfamiliar style or formatting, or missing context in the email that is asking you to interact with an unfamiliar link or open an attached payment document, these are all red flags and should not ignore them.

How Long and Complex Should a Password Be?

With computing power increasing, the ability to crack passwords quicker has made the days of 8- or 12-character length passwords outdated and MFA more critical than ever.

CISA advises that the longer a password is, the more secure it is.

To avoid creating weak passwords, make sure to include uppercase letters, lowercase letters, numbers, and special characters.

To create a password that is deemed strong enough that password strength tools say it would take centuries to crack, look to have a minimal length of 20 characters.

Creating passphrases with a combination of numbers, 4 words, and special characters can get you to this 20-character minimum easily.

Keep in mind, if you have multi-factor enabled, password complexity is not as critical because a bad actor would have to know your username, crack your password, and defeat your multi factor authentication mechanism.

This is why MFA is an absolute must on any account it can be enabled.

Yes! Anyone Can Be Scammed!

KnowBe4 Data-Driven Defense Evangelist, Roger Grimes has a LinkedIn article about how anyone can be phished or scammed.

from the LinkedIn article:

[Intelligence and "street smarts" have little to do with whether you are ultimately scammable or not. I do think being smart and "street smart" can make you less likely to be scammed in many situations, possibly most scenarios. But doctors, lawyers, engineers, successful business owners, rocket scientists, and even Nobel Physics prize winners have been successfully scammed. Many people who thought they were super street smart and unscammable have been scammed.]

KID'S CORNER

Summertime is right around the corner and Bitdefender has a great article to assist parents with navigating the cyber risks their children face. Read here.