It's phishing season!

Don't let the hackers get lucky - watch out for phishing scams.

Phishing emails are among the most common and dangerous cybersecurity threats. Key findings from a cybersecurity risk report, Proofpoint's "The Human Factor 2022," indicate that over 20 million malicious emails were sent in 2021, and over 80% of businesses were attacked in any given month.

This month's newsletter will highlight misconceptions about phishing emails. In a survey from Proofpoint for their "State of the Phish 2022" report, findings showed that more than two-thirds of respondents lack understanding about email safeguards on their work accounts. Lack of knowledge in this area presents a danger to organizations.

Misconception #1: Internal emails are always safe.

Most internal emails are safe, but that doesn't mean you can let your guard down. Hackers use email spoofing to make the email address look like it is being sent from an internal or trusted source, but it's actually a phishing email.

Tip: Go straight to the official source to authenticate or view whatever you are asked to see in the email. For example, if it looks like an email from Human Resources, go to your organization's Human Resources page to view the information and avoid the link in the email.

Misconception #2: The organization's security tools can block all dangerous emails.

Even with the best email security systems in place, some malicious emails still make it into your mailbox. Hackers will use key terms, bad spelling and other tactics to bypass security protocols. Every email that makes it to your inbox needs to be reviewed carefully.

Tip: Be suspicious of supposedly official emails using bad spelling or grammar.

Misconception #3: Emails with familiar logos and contact information are safe.

It can be tough to spot a phishing email, but it's easy to spot a familiar logo. Hackers will simply download a familiar logo and attach it to a malicious email. If it is a trusted brand, people are more likely to let their guard down and provide information.

Tip: Look out for generic "Dear customer" greetings — this is a hacker's go-to!

Misconception #4: If you receive multiple emails from someone, it must not be a hacker.

Not all phishing emails are created equal. Hackers will get hold of someone's email and strike up a business-related conversation to talk their way into the system. This type of phishing attack is called Business Email Compromise and is often used on executives or employees with access to financials or sensitive information.

Tip: If someone reaches out to you, confirm their identity with a third party before giving them any information!

Conti: One of the world's most successful and ruthless ransomware groups stopping at nothing to cause disruption.

Conti has shown their power in recent attacks. Over the last year, they have attacked healthcare services in the US and Ireland, a sector traditionally considered off-limits. They have been known to attack public schools and even popular snack brands, interfering with ordering and dispatch of products.

Cybersecurity roles — Privacy manager

Have you ever wondered what your friendly cybersecurity team is up to? We'll share a cybersecurity job role each month to give you an inside look!

Privacy manager

A privacy manager is responsible for the development, creation, maintenance and enforcement of the privacy policies and procedures for an organization. They ensure compliance with all privacy-related laws and regulations. The privacy manager takes an active lead role when a privacy incident or data breach occurs: they start the investigation, monitor progress and resolve any privacy issues. They also build privacy programs for their organization that minimize risk and ensure information confidentiality.

E-TECH