IN THE NEWS

Butzel attorneys answer Q&A in *Corp! Magazine* on the topic of phishing

Corp! Magaizine
4.14.2021

Related People

Claudia Rast
Shareholder

Related Services

Cybersecurity and Privacy Specialty Team

Emerging Technology Specialty Team

Phishing attacks are one of the most common—and effective—forms of social engineering. These attacks attempt to convince a person to do something by impersonating a known party, such as friends, colleagues, or a company.

These seemingly legitimate requests ask the user to take some type of action, such as clicking on a link or opening a document. Phishing campaigns focus on sending out high volumes of generalized emails with the expectation that only a few people will respond.

Identifying phishing email
Phishing attacks work because they focus on simple human curiosity as opposed to other types of cyber-attacks that are bot driven and target software vulnerabilities. In the basic phishing attack, a social "engineer" may say or claim that:

- They've noticed suspicious activity or log-in attempts (which they will fix if you click here...)
- There's a problem with your online account or payment information (just enter your credential here...)
- You have to confirm some personal information (just enter it here...)
- The attached invoice needs confirmation (open it to confirm your order)
- You need to make a payment (just go to this link)
- You're eligible to register for a government refund (click here to find out how much)
- You're eligible for a free product (click here to see what that is)

In all instances, these emails will include a link or attach a document that will carry a malicious payload. Once clicked or opened, the malware will take over.

What do you do if you inadvertently click on the link or open the document? Time is of the essence here. Shut down your computer completely and call your IT Department.

Click here to read the full article.