PHISHING - A Review and some Numbers...

Phishing is a type of cyber attack where attackers randomly send emails to a broad audience in an attempt to trick people into providing sensitive information such as account credentials, personal details, SSN's etc.

Targeted email, or spear phishing, is reported by businesses to be used in 91% of successful data breaches and 95% of all enterprise networks

Phishing's Top Delivery Mechanisms...

Over 150 million "phishing" emails are sent EVERY DAY

66% of malware is installed via malicious email attachments

Fake invoices are the #1 disguise for distributing malware

The most common malicious attachment types:

- Office 38%
- Archive 37%
- PDF 14%

83% of global IT Security respondents experienced phishing attacks in 2018, an increase from 76% in 2017

56% of IT decision makers say targeted phishing attacks are their top security threat

30% of phishing messages get opened by targeted users and 12% of those users click on the malicious attachment or link

Only 3% of targeted users report malicious emails to management

Credential compromise rose 70% over 2017, and they've soared 280% since 2016

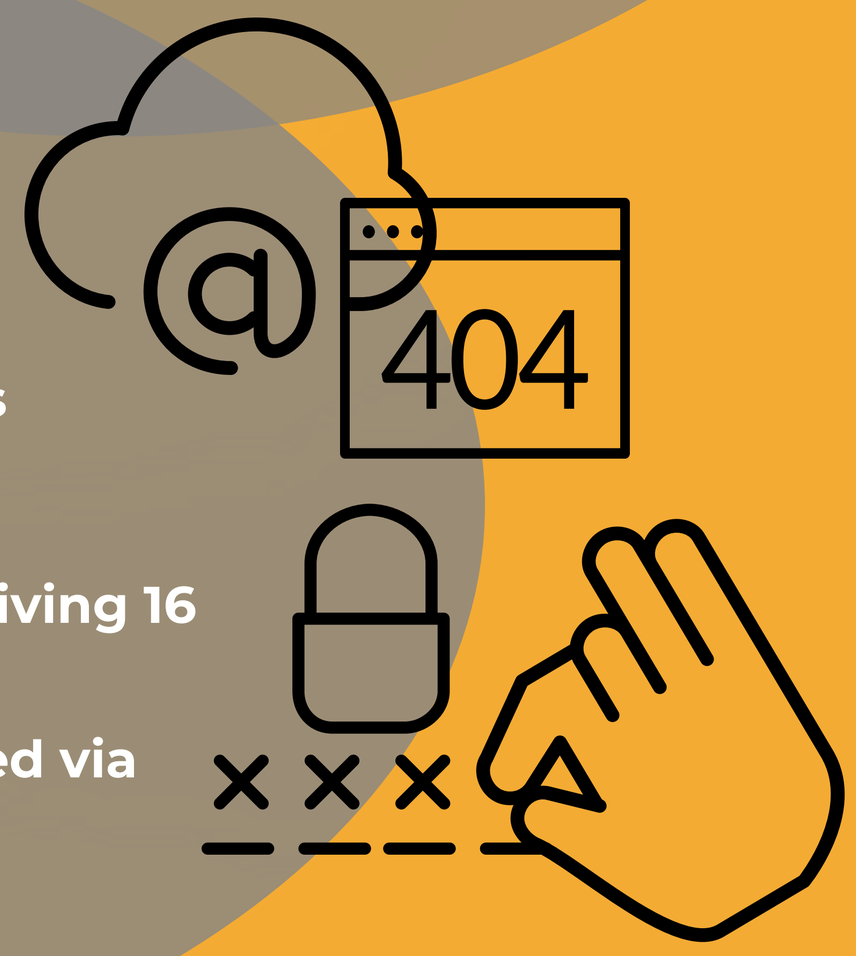
Business email compromise (BEC) scams cost organizations $676 million in 2017

CEO fraud is now a $12 billion cost to business

50% of phishing sites now using HTTPS

By the end of 2018, the average user was receiving 16 phishing emails per month

49% of non-point-of-sale malware was installed via malicious email



More Information? Call Us... 877 308 9167

www.idresolution.net

idresolution
Your Identity at Risk, Our Solutions at Work™