INFOSEC EXPOSED

Jun 2022

geevo® - delivering positive change!

INSIDE

Our contact details

Tel: +357 24 023203

Email: info@geevo.eu

Visit us: www.geevo.eu

NEW FINDINGS THIS MONTH

By Constantinos Andreou, Cyber Security Engineer

Phishing: If you suspect deceit, hit delete!

Phishing Readiness will condition your employees to become less susceptible to malicious phishing attacks by creating and launching custom phishing simulations.

How does it work?

- Send phishing emails to your employees
- Track and report on who opens and clicks on links in the email
- Deploy online training to employees that 'fail'
- Re-send the phishing emails on a regular basis to monitor improvement

Speak to our Cybersecurity experts!

PHISHING METHODS

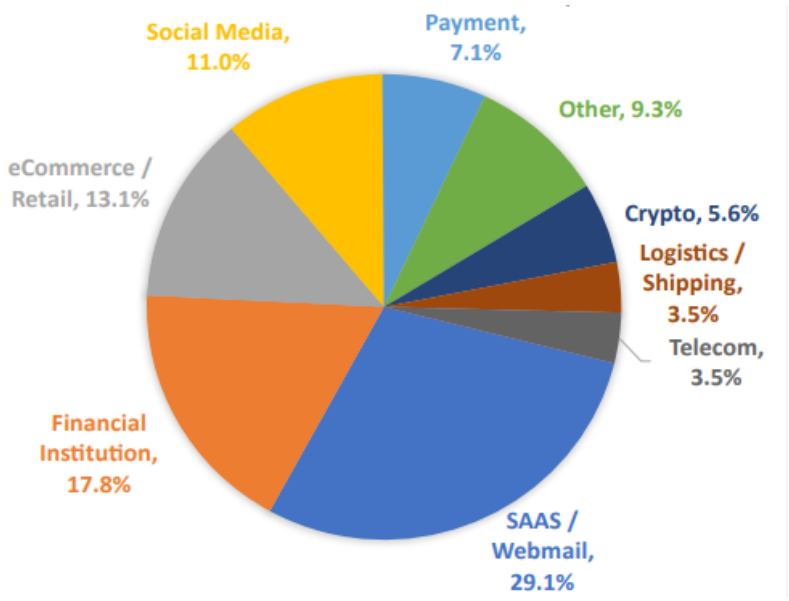
Email & SMS Phishing: Scammers disguise malware and spyware as email attachments and add links on the email/sms message body to direct users to fraudulent websites, to phish for financial information through marketing campaigns or even fake invoices.

Search Engine Phishing: Scammers tend to rely on users' trust of search engine results to create fake sites offering different products or even services to collect personal payment information.

Malvertising: A scammer inserts malicious code into online advertisements so when users click on that specific add, their device will be infected with malware.

Vishing: Scammers tend to use VoIP to spoof the caller ID and impersonate another person or company to gain access to sensitive information of an individual.

MOST TARGETED INDUSTRIES OF PHISHING ATTACKS IN 2021



What you will expect

- **Raise user awareness:** A phishing email simulation will raise user awareness on the different phishing email threats which exist online.
- **Lower the risk of exposure of the company:** More educated users on phishing means less of a risk for the company to be exposed to data leakages or even a complete downfall.

THINK WE CAN DO THIS TOGETHER? GET IN TOUCH.