SOCIAL ENGINEERING INDICATORS

Most cybercriminals are master manipulators, but that does not mean they are all manipulators of technology — some cybercriminals favor the art of human manipulation. They favor social engineering, which means exploiting human errors and behaviors to conduct a cyberattack. Don't be the next victim - watch out for these signs of a phishing email!

SUSPICIOUS SENDER'S ADDRESS

Cybercriminals will often imitate the address of a legitimate business when sending you an email or a message.

GENERIC GREETINGS AND SIGNATURE

Generic greeting like "Dear Valued Customer" or "Sir/Ma'am", combined with a lack of contact information in the signature block are suspicious.

SECONDARY DESTINATIONS

Some phishing attacks involve directing the victim to a legitimate document hosting site, or attacking a non-malicious document to the message.

SPELLING AND LAYOUT

A message with poor grammar and sentence structure, misspellings, and inconsistent formatting is most likely a sign for a possible phishing attack.

SPOOFED HYPER-LINKS & WEBSITES

Spoofed links do not match the text that appears when you hover over them. Malicious websites use a variation in site's spelling or a different domain.

SUSPICIOUS ATTACHMENTS

Often, cybercriminals use a false sense of urgency or importance to persuade the user to download/open a malicious attachment.

Source: Cybersecurity and Infrastructure Security Agency (CISA)

Familiarizing yourself with these Social Engineering indicators will help you identify and report them to your cybersecurity team!

How can we help you?
Get in touch to find out more about our services

SoftwareONE AG
Riedenmatt 4
CH-6370 Stans

T. +41 44 832 41 69
E. info@softwareone.com
W: cybersecurity-user-awareness