Aon | Professional Services

In deep water: phishing risks for professional services firms – executive summary

Ransomware is a leading risk for professional service firms in 2021 – ***Aon's Cyber Solutions Group*** *statistics show that ransomware attacks have increased* ***486% in two years****.*

- Attackers are very sophisticated
  - They employ behavioral psychologists
  - They employ professional translators
  - They do their research and know:
    - You (they have your name, email address, and photograph)
    - Your clients
    - Your expertise, experience, and specialty
    - Personal information shared on social media (from where you live, to your dog's name, including information leaked on the dark web, including SSN's)
    - Your colleagues
    - Your position in your organization – who you report to and who reports to you
    - Your vacation schedule and where you go
- Attackers have all the information they need to
  - Craft convincing messages
  - Impersonate you to someone else (e.g., a client)
  - Impersonate one of your clients or vendors to you
  - Convincingly emulate a prospective client
- The pandemic and subsequent shift to remote working environments has given the attackers new opportunities to exploit issues with carefully crafted messages
- Statistically, attackers need to send only 20 messages to have a high chance that at least one person will click a link or open an attachment, potentially releasing malware into your systems
- You and your employees are the "gatekeepers"
  - When they get past you, everything else is technology and they are very, very good at technology
  - The attackers only need to be lucky once
  - Your best defense is training the gatekeepers, often and repetitively

Release Date: May 2021

Empower Results®

What can you do?

- Be vigilant – look out for spoofed emails and names that are not quite right
- Think twice before opening documents or clicking on links
- Double-check changed instructions using “out of band” communication with parties to a transaction
- If you think you have a problem, tell someone – the sooner the better
- Establish and follow protocols – changes and exceptions are always red flags