Aon | Professional Services

In deep water: phishing risks for professional service firms

*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**.*

Click here for the Executive Summary

How Real is the Threat?

A recent report from Coveware, a leading extortion negotiator, shows that professional services is now the most-targeted sector of the economy, accounting for over 25% of ransomware attacks. That is more than the next two sectors combined -- Public Sector at 11.6% and Healthcare at 11.3%.

The reasons professional service firms are so attractive to attackers are simple:

- Attackers know that professional service firms host very valuable data
- Professional service firms are perceived as "wealthy" and able to pay to keep sensitive client data out of the public domain
- Attackers know that professional service firms are risk averse and purchase insurance

How do the Attackers Operate?

There are three main types of attacks: generic phishing, spear-phishing and "man in the middle" attacks.

Generic Phishing is characterized by messaging (usually email) that is targeted at a broad population using email addresses harvested from the firm's website. The messages vary in style and substance but most often play on "FUD" (Fear, Uncertainty, and Doubt), "FoMo" (Fear of Missing Out), and hope. In the remote-working environment, these messages can be very attractive to employees who feel disconnected from their organization, are fearful about their future, are looking for opportunities to connect with others, or are hopeful of a bonus, promotion, or any other good news.

As a result, an invitation to click on a link or open an attachment is often accepted, particularly if it is well-constructed and appears to come from a trusted source. These messages tend to be disguised as information about:

- Bonus and promotion announcements
- Office opening timing and procedures
- Reductions in staffing / layoffs
- Mergers
- Formal or informal gatherings
- Competitions and prizes
- COVID information – e.g., vaccine availability and timing

Release Date: May 2021

Even in a well-trained workforce this type of messaging is successful **approximately 5% to 20% of the time (depending on "template" type)**. In practical terms, this means that if attackers send as few as 20 emails there is still a high chance of at least one successful click on a tainted link.

The tainted link often is used to introduce a highly automated form of malware into the firm's computer systems. This malware will then map the network, detect vulnerabilities, and report back. The attackers can then use "hands on keyboard" to navigate through the network and attempt to secure a level of control that enables them to steal data and plant ransomware. This process can take anywhere from days to months, but the hackers are patient, driven by the expectation of a substantial payoff from their efforts.

Spear-Phishing is a carefully crafted process of targeting a high-level individual within the firm, usually one with authority to facilitate a deal or a financial transaction. Spear-phishers extensively research their target using publicly available information (particularly social media) and stolen information from the dark web to build up a profile on the individual, including information on friends and colleagues.

The individual is then targeted with messaging designed to facilitate a particular objective. Such campaigns have been successfully employed in some very substantial frauds, where sophisticated executives and partners have been duped into authorizing payments of millions of dollars, believing that the fraudsters were legitimate clients, vendors, or executives of the firm.

"Man-in-the-middle" attacks are possibly the most insidious and difficult to prevent. The hacker typically uses social engineering to break into the email account of one of the participants in a major deal. The favored type of deal is one involving multiple parties and an escrow agent.

Having infiltrated the email system, the hacker reviews emails relating to the transaction, learns the timeline of the deal and the names, authority levels, and responsibilities of the participants, and studies the modes of address and writing style of the person whose email they have hacked.

At a convenient point, the attacker will "hijack" the email traffic about the deal and its participants by setting up automatic rules to divert all sent and received email to a hidden folder. The hijacker then takes over the correspondence and at the right moment issues instructions for payment to a fraudulent bank account.

Since the hacker is using a legitimate email address, has access to all the details about a transaction, and mimics the writing style of the individual they are impersonating, these attacks are particularly difficult to detect and prevent.

The defense of your firm

The **FBI Internet Crime Complaint Center (IC3) 2020 Internet Crime Report (March 2021)** includes information from 791,790 complaints (an almost 100% increase from 2019) and reported losses of $4.2 billion.

The top three crimes reported by victims in 2020 were:

- phishing scams
- non-payment/non-delivery scams, and
- extortion

Victims lost the most money to business email compromise scams, romance and confidence schemes, and investment fraud. The IC3 also received over 28,500 complaints by both businesses and individuals involving scams exploiting the COVID-19 pandemic.

There are many technological solutions that help reduce the amount of fraudulent email that will reach a user's inbox and that identify and strip out malware-laden attachments. However, tools are not 100% foolproof. As attacks continue to become more sophisticated, there will always be some fraudulent and phishing email that will get through technological defenses. Opening just one document or clicking on just one link sent in one of these emails could be the first step in a serious and ongoing problem.

The best defense is training the firm's employees on cyber safety, frequently and repetitively. Employees are typically the weakest link in the chain or the strongest defense against attackers. Every employee must understand and remember:

- The threat is very real and very personal – the hackers are targeting YOU
- Attackers are sophisticated; they do their research and their phishing emails are crafted to be plausible and convincing
- Attackers are relentless and only need to be lucky once
- You have a lot of technological protections in place both at the perimeter and inside the firm's network, BUT
    - Once the attackers are in the network, they have good technology, too
    - The best protection is not to let them in at all

What can you do?

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