Cyber Risks & Liabilities

Third Quarter 2020

3 Common Phishing Attacks and How to Avoid Them

A significant number of organizational data breaches stem from phishing attacks. At a glance, these attacks result from a cyber criminal utilizing a fraudulent email or other form of communication to trick the victim into providing sensitive information or downloading malicious software on their device. Phishing attacks have become increasingly sophisticated in recent years and can take place in a variety of different formats.

What's more, the consequences of such an attack on organizations like yours can be severe—including lost or stolen data, prolonged business interruptions, financial devastation and reputational ruin. With this in mind, it's crucial for your organization to understand the most common types of phishing attacks and implement strategies to reduce your risks.

Review the following for an overview of three top forms of phishing attacks and steps that your organization can take to protect against them:

1. **Deceptive phishing**—Known as the most common type of phishing attack, deceptive phishing occurs when a cyber criminal impersonates a trusted organization (e.g., a bank) via email to fool the victim into providing sensitive data or login credentials. To prevent deceptive phishing attacks, instruct staff to avoid responding to emails from seemingly legitimate organizations if the message appears overly urgent or aggressive, contains a generic greeting or has spelling errors.
2. **Spear-phishing**—This type of phishing attack entails a cyber criminal sending a more customized email (e.g., using the victim's name or job title in the greeting) to convince the victim to click on a malicious link or attachment. To avoid spear-phishing attacks, discourage staff from sharing personal or company information online, and consider investing in security software that analyzes incoming emails for harmful links or attachments.
3. **Whaling**—This form of phishing attack takes place when a cyber criminal specifically targets a company executive with a spear-phishing email, gaining access to the executive's account or device and authorizing fraudulent financial transfers or the distribution of employees' personal information. Reduce the risk of whaling attacks within your organization by requiring executives to complete the same cyber security training as the rest of your staff and implementing multifactor authentication for all financial transactions and data transfers.

For additional guidance on how to mitigate your organization's cyber exposures, contact us today.

What Does Cyber Insurance Cover?

Across industry lines, organizations have become increasingly reliant on workplace technology to conduct key business operations. Whether it be for communication purposes, e-commerce, or data collection and storage, continued technological advancements have helped streamline a variety of organizational processes.

Nevertheless, utilizing such technology and digital practices within your workplace carries additional cyber exposures and liabilities. All it takes is a single security failing to cause large-scale damages, leaving your organization to deal with the costly ramifications that accompany a data breach. That's why it's crucial to secure adequate cyber insurance.

Specifically, having a cyber liability insurance policy in place can help protect your organization against financial losses that result from a data breach or other cyber incident. Cyber liability insurance typically includes the following types of coverage:

- **First-party coverage**—This form of coverage can offer protection for any losses that your organization directly incurs from a cyber incident, including:
    - The cost of replacing or restoring any lost, stolen or damaged electronic data
    - Income losses and extra expenses that result from disrupted business operations
    - Ransom payments from a cyber extortion incident
    - The cost of notifying any parties affected by a cyber incident
    - Reputation preservation expenses (e.g., any public relations efforts following a cyber incident)
- **Third-party coverage**—This form of coverage can provide protection for claims made or legal action taken against your organization by any stakeholders that suffered losses due to your company's security failings, including:
    - Claims regarding negligent acts, errors or omissions that caused a cyber incident
    - Legal investigation and defense costs that result from a cyber incident
    - Regulatory fines or penalties due to noncompliance with data protection laws

Don't let your organization suffer the costly consequences of a data breach. Contact us today to secure a cyber liability insurance policy that meets your organization's unique needs.

Top Reasons to Secure Cyber Insurance

Many organizations incorrectly label cyber insurance as a luxury purchase rather than a necessity. In fact, a recent survey conducted by insurance experts found that nearly 60% of small and midsized companies don't have any type of cyber insurance. What's worse, less than 30% of those companies feel inclined to purchase a such a policy in the near future.

Despite these startling statistics, it's vital for organizations of all sizes and sectors to secure adequate cyber insurance. Here's why:

- **You can't afford a lack of protection.** A single cyber incident can cost your organization millions of dollars in recovery expenses, business interruption costs and legal fees, which—without an insurance policy in place—could cause financial devastation.
- **Cyber attacks are common.** Don't assume that cyber incidents are a rare occurrence. Especially as cyber criminals become increasingly sophisticated and organizations continue to digitize key business operations, data breaches have become a top threat—making cyber insurance all the more critical.
- **Coverage is a contractual requirement.** Many clients, vendors and suppliers include cyber insurance as a requirement in contractual agreements. In other words, securing cyber insurance is crucial to maintain your supply chain and ensure solid customer relationships.
- **Noncompliance can be costly.** In the event that you violate state, federal or international data protection laws, the resulting fines can be significant. Cyber insurance can assist you with these costs.