CYBER CRIMES SPIKE AS PROFESSIONALS, BUSINESS OWNERS WORK FROM HOME

AHT INSURANCE
A BALDWIN RISK PARTNER

The coronavirus pandemic sent millions of professionals to work remotely and dramatically shifted work patterns over the last year. While CEOs, COOs and other C-suite-level employees, business owners, financial advisors and family office professionals were reconfiguring their home offices, cyber criminals were busy honing their nefarious skills to access confidential and proprietary information, outsmart individuals into falling for fraudulent wire transfer scams and take computer network systems hostage via malware in exchange for money. Through the COVID-19 pandemic, bad actors have been increasingly successful with a wider target to attack, as more individuals became reliant on digital technology for business amid weakened cyber security measures in a work-from-home environment.

Incidents of social engineering, including phishing and vishing, along with ransomware saw significant spikes during 2020. For example, social engineering attacks increased from 46% in 2020 Q1 to 60% by Q2 2020. The pandemic also sparked a 72% ransomware growth and mobile vulnerabilities grew by 50%.*

INSIDE SOCIAL ENGINEERING

Cyber criminals manipulate human error using social-engineering techniques to gain confidential information and commit theft or fraud. For example, phishing attackers pretend to be a trusted institution or individual in an attempt to persuade the target to expose personal or business data or wire transfer money.

Vishing (voice phishing) involves scams designed to get an individual to reveal banking and other confidential information over the phone. One particularly dangerous scam is designed to thwart two-factor authentication with scammers calling individuals to say they are conducting a security check. The cyber criminals will ask for the code sent to an individual's phone; if the code is provided, the scammer can take over the account. One of the reasons that vishing can be very convincing is that typically scammers will use spoofed caller ID numbers that look legitimate.

INSIDE RANSOMWARE

The FBI has warned that the huge shift to remote work created the perfect breeding ground for cyber criminals to target workers. Cyber criminals research high-net worth individuals, companies, and organizations through publicly available information to create a profile of the victim that can include name, address, position, email address and other relevant information. They then create realistic-looking websites that may even include a company's logo to convince victims they are from the company's IT department. In many cases, the criminals will tell the victim that the company is switching VPN providers and they need to go to this new website to connect to the company network securely. What they're actually doing is capturing login credentials, so they can access the company network and launch malicious software code to block people or organizations from accessing their computer systems until a ransom has been paid. Cryptocurrencies, such as bitcoin, have made it easy for these bad actors to receive payment without exposing their identities.

BEEF UP CYBERSECURITY AT HOME, AT WORK, IN THE FAMILY OFFICE

To stem the rising tide of cyber threats with more individuals working from home, professionals and all employees should implement the following measures:

- Maintain good password hygiene, including using complex passwords (avoid using spouse and children's names) and changing them frequently.
- Update systems and software on a timely basis, including on mobile devices.
- Use a VPN originating from a trusted connection within the organization to ensure ongoing access to corporate tools.
- Be wary of COVID-19 scams and resist the urge to click links in a suspicious email.
- Avoid using work devices for personal matters.
- Recognize the signs that your computer is affected and contact IT immediately.

Employers and family offices should put the following risk-management measures into practice to mitigate cyber-related losses:

- Meet regularly (including virtually) with your IT staff to identify vulnerabilities as a result of more employees working remotely. Prioritize protecting your most sensitive information and business-critical applications.
- Alert all employees, especially those in accounting, finance, HR, and benefits, to the types of social engineering scams being perpetrated to get them to wire transfer funds or disclose confidential and sensitive information.

- Set up an out-of-band verification process to confirm the identity of the person requesting a wire transfer, a change to banking information or payment instructions, or access to sensitive data, such as tax and payroll information. This includes:
    - Requiring voice verification for all changes involving banking information.
    - Not relying on the contact details provided in the request, including a phone number to call in the email.
    - In lieu of using "Reply," forward the email and type in the email address you know to be correct.
- Advise clients you will not change banking instructions without authentication and to treat any such request as possibly fraudulent.
- Ensure your employees understand to whom they should communicate about any suspicious activities.
- Make sure all business-owned or managed devices are secure, and extend the same network security best practices that exist within your organization to all remote environments. These practices include:
    - Securely connecting users to their business-critical cloud and on-premises applications, such as video teleconferencing applications
    - Protecting laptops and mobile devices, including VPN tools with encryption; ensure that the latest versions of VPNs are used, and patches are applied promptly
    - Enforcing multi-factor authentication (this is typically a password followed by a code sent to an individual's phone)
    - Ability to block exploits and malware
    - Ability to filter malicious domain URLs to thwart common phishing attacks.
- Employ a regular backup system with files stored remotely.
- Ensure that the security settings for cloud-based services are appropriately configured.

A cybersecurity program should also include an incident response plan and insurance. Companies and family offices need to be prepared to effectively respond to a cyber incident, which includes resuming business operations with minimal impact and demonstrating to investors, employees and other parties that the incident was resolved appropriately. Cyber insurance can be designed to respond in the event of an incident for the following:

- Forensics fees to determine how the attack occurred and to what extent
- Notification costs if there is a breach of third-party confidential information
- Crisis management and public relations expenses to protect one's reputation
- Remediation costs
- Ransomware payments
- Fees and liability settlements in the event of litigation
- Business interruption/loss of income as a result of the cyber event
- Other related expenses

Cyber insurance policies differ significantly and require professional expertise to ensure the right policy is put into place. The AHT Private Risk Management team can help protect your legacy and business with a tailored cyber and risk management program that addresses your risk profile.

ABOUT AHT

AHT Insurance is an insurance brokerage and consulting firm offering property and casualty, employee benefits, retirement, private client and international services for clients throughout the United States and 42 other countries. Supporting numerous industries and boasting national recognition in the technology, manufacturing, government contracting and nonprofit practice areas, AHT offers clients highly customized solutions to identify and help mitigate risks they may face. AHT's professionals put clients' needs first and focus on what they do best – providing best-in-class service and solutions. Learn more about AHT at ahtins.com.

*Sources: *Beazley, FBI, Kapersky, EY*