CASE STUDY

Solo Practitioner Law Firm Curbs Social Engineering Scam

INDUSTRY
Legal

EVENT TYPE
Social Engineering

EMPLOYEE COUNT
1-25

LOCATION
Florida

KEY COVERAGE
Breach Response

POLICYHOLDER QUOTE
"The good news is Coalition showed up right away and gave me the information that I needed to stop the problem from getting worse."

— Attorney, U.S. policyholder

When a Florida-based lawyer powered up his computer and noticed a small black box on his desktop, he immediately suspected something was wrong.

A few days prior, the attorney had installed a surveillance system at his new office but was unable to sync all of his devices. After a quick online search for tech support, he was connected to a representative and granted them remote access to his computer to fix the issue.

The representative told the lawyer that his computer had been infected by foreign threat actors and offered to remove the malware for an additional fee. Soon after paying for the additional security services, the attorney noticed the small box at the bottom of his computer screen "running some sort of code that was moving fairly quickly." That's when he realized he'd been scammed.

The lawyer contacted his insurance agent, who immediately connected him with the Coalition Claims Team. We advised him to immediately shut down his computer as a precaution and recommended a digital forensics investigation.

A security analyst with Coalition Incident Response (CIR), who happened to be nearby, offered to visit the lawyer's office and assist with data preservation in person. After restoring the data through an external drive and searching for indications of ransomware, CIR found no evidence that threat actors accessed any sensitive data.

During the investigation, CIR determined that the lawyer clicked on a fraudulent website while trying to set up his surveillance system as part of an attack known as SEO poisoning. The small black box on the lawyer's desktop only contained a "dummy" script, intended to simulate a malware infection and scare the lawyer into calling tech support again for additional services.

CIR advised the lawyer on steps to reduce his risk in the future, such as using a password manager and implementing multi-factor authentication.

One key coverage helped the lawyer through this social engineering scam: Breach Response covered the cost of CIR's investigation, which totaled $24,500.

Lesson Learned: Be Wary of Clicking on Search Results

Individuals have rightly grown more wary of clicking on links and attachments sent via email, but that's not the only place threat actors try to trick victims. Threat actors are capitalizing on the blind trust we put in search engine results and hide malicious websites in plain sight. Businesses should include SEO poisoning in security awareness training and encourage the use of password managers so that if a user goes to a website and credentials don't autofill, it sets off alarms. In addition, web security tools can be implemented to identify and prevent websites from serving malicious content, and endpoint security solutions can identify and block attempted infections by malware delivered by SEO poisoning attacks.