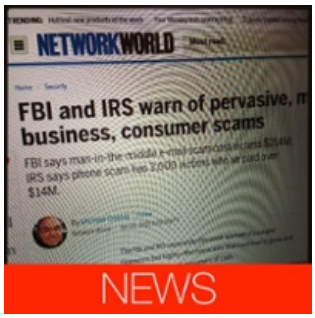
Wait, don't pay that invoice! You might be keeping a crook in business.

Find me on:

Jan 27, 2015



NEWS

The FBI has issued a warning about a scam that tricks employees into paying invoices that appear legit, but are actually fraudulent. This scam, named the Business E-mail Compromise Scam (BEC), has caught the U.S. Government's eye because of its increasing popularity.

In the past 14 months, reported victims of BEC rip-offs have lost over $200 million. And remember that as my co-founder wrote in Forbes last year, when a business is the victim of wire fraud, you can't always count on the banks making good again.

How it works

In one version of the scam, criminals learn who your company's vendors are. They do this in a variety of ways, including spyware installed during an employee's work or personal browser session. Once the thieves know your vendors they spoof those firms' email addresses and invoice payment from you.

In another scenario, the scammer either spoofs or hacks into the account of your CEO or other senior officer. From that account the thief sends a message to an employee, asking them to pay to a vendor's invoice. The email includes a link to complete the payment, but that link transfers the money straight into a criminal's bank account.

In the third version of the BEC scam, the personal email of your vendor's employee is hacked. The criminal then sends emails to you and the vendor's other customers, invoicing for payments. Again, the payment links in the emails are connected to the crook's bank account.

The second and third scenarios described above are especially scary because the email account requesting the fraudulent payment might be a completely legitimate address.

We all know crooks are getting smarter. Using complicated methods they can learn the details of your vendor relationships and hide behind the email account of anyone in your company. To pull off scams like BEC, criminals often hack browsers as a starting point to gain information and slither into your network.

Protect ya neck!

Keep in mind, it's not just your work machines' browsers that leave your company vulnerable. Your employees use their personal computers' browsers to do work. It's this combination of personal browsing at work and work browsing on personal machines that puts your network and email accounts at risk. Your responsibility to protect your network also includes helping staff be safe on their personal web sessions and email exchanges.

One solution is education and training. Teach workers to check sender email addresses and keep an eye out for unusual invoice requests. In addition, we recommend creating a protocol of telephone or face-to-face verification before someone pays an invoice, and many websites will offer 2-factor authentication to add another layer of security.

A technology solution is also essential -- something that safeguards your staff's connection to the Internet both inside and outside the office. This can be accomplished by installing a secure browser that serves as the exclusive link to your business

apps and email. Secure browsers insulate potentially dangerous web code in a sandbox, preventing infection from malware. It's even better if your secure browser stores long, complex, encrypted passwords in a lockbox in the cloud, rather than on employees' local hard drives. The browser should also delete cookies (and malware) the moment the Internet session ends.

Secure browsers are ideal, but some folks at your company might prefer to continue using their familiar old browsers. No problem. That challenge is solved with a secure cloud-based browser that seamlessly launches only when those employees link to a work account or launch a business app. Your staff are happy because they can do most of their surfing in their favorite browsers. Meanwhile, your network stays secure.

When it comes to keeping track of scams, the FBI's updates are invaluable. Yet some firms won't heed the warnings. They'll soon find themselves victims of BEC and other ripoffs. Luckily, you can take steps to make sure you're not one of them.

Topics: News