Funds Transfer Fraud Increasingly Affects Small Firms

While ransomware is making the headlines as the major cyber threat for businesses, small and mid-sized organizations are increasingly being targeted by lower fraud that dupes them into wiring criminals funds, according to a new report.

These funds transfer fraud crimes involve hackers gaining access to a company's mailbox and extracting payments that go into their accounts through a variety of techniques. Worse, by the time a company realizes they were scammed, the money is long gone and the bank accounts are closed.

It's imperative that companies have in place proper systems safeguards to combat these attacks, and that includes regularly training staff on how to identify these attempts to steal funds.

Losses from funds transfer fraud increased 69% for U.S. businesses between 2020 and 2021, according to cyber insurance and security firm Coalition's "2022 Cyber Claims Report."

But smaller and mid-sized companies saw attacks surge even more. Average initial losses from funds transfer fraud for small firms (those with less than $25 million in annual revenue) more than doubled to $309,000 in the second half of 2021, compared to the same period in 2020.

Additionally, enterprises with between $25 million and $100 million in revenue saw a 68% increase in the frequency of funds transfer fraud.

How it works

Criminals will often try to penetrate your servers by sending "spearphishing" e-mails. These messages look like they're from a trusted sender to trick victims into revealing confidential information. That information lets criminals access company accounts, calendars, and data that gives them the details they need to carry out the scheme.

They may also send malicious e-mails in the hope that an employee clicks on a bogus link. The link then releases malicious software that infiltrates company networks and gains access to legitimate e-mail threads about billing and invoices.

Once the criminals have access to your business mailbox, they can manipulate your contacts and modify payment instructions, sometimes without even triggering any security alerts.

One of the most common ways this is done is a criminal sending e-mails that appear to come from a known source making a legitimate request, like in these examples:

- A vendor your company regularly deals with sends an invoice with an updated mailing address. But it's a scam and the new address is bogus.

- A vendor sends change-in-payment instructions that purport to come from a customer or vendor via a lookalike e-mail domain (sometimes criminals will compromise a customer or vendor's e-mail system and send your organization an invoice).
- A company CEO asks their assistant to purchase dozens of gift cards to send out as employee rewards. She asks for the serial numbers so she can e-mail them out right away. But the request is from a fraudster.

Protecting your enterprise

The Federal Bureau of Investigation recommends that all organizations follow these tips to reduce the chances of being hit with wire transfer fraud:

- Don't click on anything in an unsolicited e-mail or text message asking you to update or verify account information. Look up the company's phone number on your own (don't use the one a potential scammer is providing), and call them to ask if the request is legitimate.
- Carefully examine the e-mail address, URL, and spelling used in any correspondence. Scammers use slight differences to trick your employees and gain your trust.
- Be careful what you download. Instruct your staff to never open an e-mail attachment from someone they don't know, and to be wary of e-mail attachments forwarded to them.
- Set up two-factor (or multi-factor) authentication on your accounts.
- Verify payment and purchase requests in person if possible, or by calling the person to make sure it is legitimate. You should verify any change in account number or payment procedures with the person making the request.
- Be especially wary if the requestor is pressing you to act quickly.

Insurance options

The best option for coverage is a commercial crime insurance policy. Most of these policies cover acts like:

- Employee dishonesty
- Computer and funds transfer fraud
- Forgery or alteration
- Money and securities theft
- Theft of client's property.

Some policies may exclude funds transfer fraud, or they may have lower sublimits for such acts. In such cases you may need to get a policy extension to cover the risk.

There is also cyber liability insurance, which covers direct losses resulting from cyber crime. But these policies will often exclude coverage for social engineering attacks, which are the kinds that the criminals behind funds transfer fraud use.

You may be able to purchase a rider to your cyber liability policy that would cover these crimes.

###