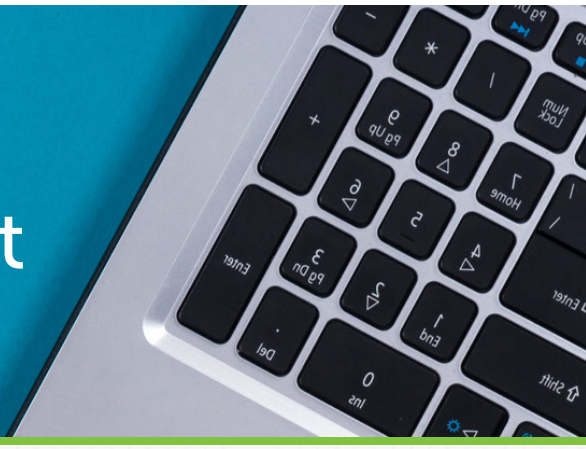
Click Thinking Spotlight

Account Takeover and Lateral Phishing



Account takeover and lateral phishing are so effective because they provide cybercriminals with a perfect cover for their scams: legitimate business email accounts that have been compromised for their use.

- Scammers research target companies using information found easily on the internet through web searches and professional and social networking sites. Using this information, they send phishing emails to their targets in the hope they'll click on a link that secretly gives them access to their account and network. Once they're in, the account takeover begins.
- Scammers can now set their sights on any intel of value that can be leveraged to suit their needs. They'll learn about the company's business practices, relationships, email signatures, financial transaction processes, and move throughout the network compromising as many accounts as they can. This process is called pivoting.
- Armed with the accounts and information they need, the cybercriminals craft and send phishing emails designed to distribute malware, facilitate wire fraud or perpetrate other scams. And because these attacks come from inside from legitimate email accounts, they're very difficult for recipients to detect.
- A successful attack results in a transfer of money from the victim to the criminal who often continues scamming undetected under legitimate-looking cover. As such, you can see how the takeover of one account can expand to more, with the cycle of intelligence gathering and scamming repeating and growing if it goes undetected.
- Lateral phishing, an offshoot of account takeover, occurs when compromised accounts are used to scam others within the accountholder's network. The victims are typically business partners or vendor companies who rarely suspect their legitimate email contact is a scammer in disguise.
- Because of this, lateral phishing attacks tend to have a high success rate. In a recent study, researchers found that one in seven organizations has experienced a lateral phishing attack.
- These attacks, targeting a wide range of victims and organizations, can be extremely damaging to a business's brand reputation, especially if they lead to additional widespread attacks in other organizations.
- A robust information security culture and a skilled information security firm can provide perimeter, inbox and human based security in a multi-layer approach that can fortify your business against these threats.

For the Account Takeover module, see your manager or information security contact.