Security Risks from People Working from Home

(CSB20-04)

Millions of people are working from home around the world as the coronavirus pandemic spreads and authorities plead for people to stay at home to slow the rate of contagion.

Though people staying and working from home helps stop the spread of the virus, it increases the likelihood of companies getting hacked through weaknesses in employees' home networks and misuse of VPN.

"The cats are away so the mice are playing," said Karim Hijazi, CEO of Prevailion, a company that monitors cyber threats and tracks infected businesses. "The mice being malware," he added.

Chris Drake, CTO of Iconectiv, a network and operations Management Company owned by Ericsson, told Yahoo Finance that individuals and companies should expect "omnichannel" attacks: robocalls, texts, email phishing scams, and compromised apps from the App Store and Google Play.

Because people are working from home, they're also more likely to answer their phone when an unknown number calls, or be more susceptible to calls faked to look like their own phone numbers. They might think a co-worker is calling or their defenses might be down with kids at home and a general heightened level of stress.

"[Threat actors] see people in a state of worry, and that heightened emotion is perfect as an ingredient for being scammed," said Drake.

The mass work-from-home scenario might weaponize something that people view as safe: the virtual private network or VPN, which provides an encrypted connection from a computer to a network.

Hijazi describes them as "just a safe tunnel through the 'bad neighborhoods' of the internet." A VPN, for example, can't make your computer secure, it just makes the connection between you and your office secure.

This means that if a hacker compromises your computer by phishing or taking advantage of a home Wi-Fi network with weak security, the VPN can essentially turn into a direct channel for a hacker to get into an organization's network — that a company's network might implicitly trust because it's coming via a secure connection.

How to secure

- Be wary of suspicious emails, downloads, USB drives or other things that could introduce malicious software onto your computer and into the network. These could include spoofing and phishing attacks from hackers pretending to be IT personnel asking for your credentials.
- Promptly install patches and updates, including to your anti-virus software, to all devices on your home network.
- Go into your Wi-Fi router's management software to ensure it's running the latest firmware, which can update security flaws. Have a strong password on your home Wi-Fi that's unrelated to your work computer password.
- Connect to corporate networks using a secure means (e.g., a virtual private network), and store data on available encrypted network drives to avoid loss in the event of a computer virus or other malfunction.

REFERENCE

- https://finance.yahoo.com/news/surge-remote-heightens-cyber-security-195800193.html
- https://finance.yahoo.com/news/companies-faces-fresh-security-risks-due-to-people-working-from-home-192211787.html