10 WORK FROM HOME CYBERSECURITY THREATS

How has working from home changed your cyber risk posture?

1 Already Compromised

Many home networks are already infected with malware or compromised hardware that can be exploited for staging attacks, even on devices with VPN software.

2 BYOD/Mobile Security

Many companies are finding it necessary to enable remote working with personally-owned devices and mobile platforms that are not managed or secured by enterprise security solutions.

3 Unpatched Devices

Personally-owned hardware, software, and apps may not be updated or patched in a timely manner.

4 No Data Encryption

Personal devices are unlikely to use whole-disk encryption.
Online file sharing platforms may lack sufficient data encryption.
Immature key management practices can result in data loss.

5 Credential Stuffing

Attackers can compromise client-based and clientless VPN solutions using a technique called credential stuffing. This technique is particularly common when the home network has already been compromised.

10 Work From Home Cybersecurity Threats

How has working from home changed your cyber risk posture?

6 Malicious Apps

Attackers are using malicious apps in app stores as well as AWS, Azure and Office365 cloud spaces to target unsuspecting employees.

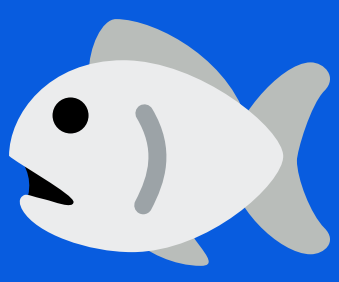
7 Backup & Recovery

Personal devices are unlikely to be configured for backup and recovery. Ransomware targeting work-from-home employees can result in significant data loss and loss of productivity.

8 Out-of-Band Collab Apps

Well-meaning employees may unwittingly expose confidential data by using communication channels like chat, messaging, video-conferencing and webcasting apps.

9 Out-of-Band Phishing



Work-from-home employees are unlikely to recognize phishing links in channels outside of email, such as social media direct messaging, chat apps, and public webcasting tools.

10 Fearful Insiders

Fear and uncertainty may cause otherwise trustworthy employees to behave differently than normal. Fearful users may transfer work files to unsecured devices, either for fear of losing their job or not being able to perform their job functions optimally.