TELEWORK
SAFE & SECURE

With today's technology and forward-thinking leaders, the steady rise of Americans working from home continues. In fact, remote work in the U.S. has grown 159% over the past 12 years[4]. While studies show that those who take advantage of a remote work environment are happier and more productive, teleworking comes with its own set of cybersecurity risks. Employees working remotely must be aware of the risks and implement proper cyber precautions.

MOST COMMON CYBER THREATS

MALWARE
Socially engineered malware are misconfigured websites that trick users into installing malware and viruses.

PASSWORD PHISHING
Spam emails that request login credentials.

SOCIAL MEDIA
False friend requests and app installations can give hackers access to your information.

ADVANCED PERSISTENT THREATS
Hackers convince users to download malware and gain access to proprietary and confidential data.

PRECAUTIONS

AT HOME:

- Use a firewall
- Use virus protection software
- Don't open unknown e-mail attachments
- Don't run programs of unknown origin
- Disable hidden filename extensions
- Keep all applications, including your operating system, patched
- Turn off your computer or disconnect from the internet while not in use
- Don't use a wireless router right out of the box—enable its security features first
- Make regular backups of critical data
- Encrypt your email

WHEN TRAVELING:

- Beware of "free" WiFi hotspots
- Use VPN access to organization network whenever possible
- Use a dedicated wireless hotspot for internet access
- If a hotspot is not available, consider tethering to a government issued cell phone

RISK REPORT & STATS

Computer virus attacks are the top type of attack reported at 33 percent of all cyber attacks in recent years.[1]

Phishing is the second most common, at 29 percent of cyber attacks.[1]

Ransomware attacks are growing more than 350% every year.[2]

Of all files, 21% remain completely unprotected.[2]

The annual cost of cyber-crime damages is expected to hit $5 trillion by 2020.[2]

65 percent of business owners admit they have fallen victim to a cyberattack[1]

In a recent poll, 32% of UK business said they had suffered a cyber attack in the past year as a direct result of an employee working remotely and outside of the organization's security perimeter.[3]

Sources: 1. Nationwide.com/CyberBlindSpots
2. CyberDefenseMagazine.com   3. ITPRO.CO.UK
4. GlobalWorkplaceAnalytics.com