# COMMON CYBER THREATS FOR REMOTE WORKERS

Whether you're working from home, a café, or another remote location, cyber threats can come from unexpected places or sources. From unsecured networks to scams that target newly remote workers who are still getting used to this new normal, it's crucial to understand how cybercriminals can target individuals working outside the office.

Cyber Attack Targets Remote Workers Should Know
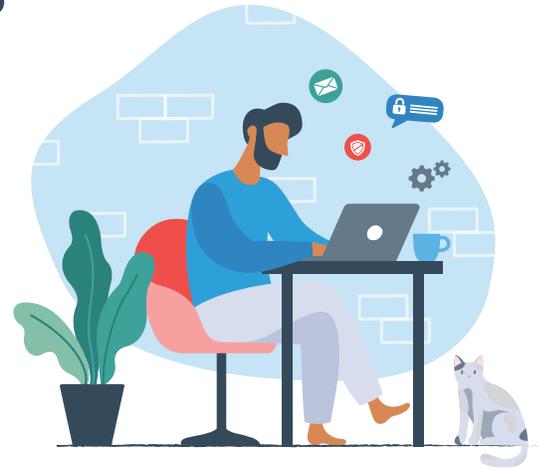
Unsecured internet connections
01

Unsecured internet networks, like open Wi-Fi in public places, are access points that forgo security features like a password or login. This absence of essential cyber security protection can make any data traveling over an unsecured network susceptible to theft or corruption.

Home Wi-Fi routers
02

Just because a Wi-Fi network, like the one in your home, has a password doesn't mean you're automatically protected from all cyber threats. Hackers can target Wi-Fi routers based on the model and internet service provider, which can expose data users may think is safe when working from home.

Weak or reused passwords
03

Remote workers who are (re)using basic or weak passwords to secure their user accounts on various platforms may be putting their confidential data in a cybercriminal's crosshairs. All it takes is a single compromised password to have an individual's identity impersonated, get locked out of an account, or have important personal or organizational information exposed.

Physical baiting or theft
04

Baiting occurs when a victim is enticed to divulge confidential data, like login credentials, in exchange for an item or good, such as a free movie or music. However, baiting via physical objects, such as a smartphone or USB stick purposely left in a public place frequented by remote workers, can also be used to steal data and other malicious cyber activity.

Emotions related to new remote work routine
05

First-time remote workers or those settling back into a new work routine may be more susceptible to scams that explicitly target individuals working outside an office environment. Cybercriminals can prey on anxieties or frustrations related to remote work to access a user's device or confidential data.

WHO CAN BE TARGETED BY THESE CYBER ATTACKS?

Any individual working remotely or an organization employing a mainly distributed workforce can be a target.

Hackers have a new favorite target, the remote worker. Cyber criminals are taking advantage of the new remote environment to target organizations through their users who may be more vulnerable. Without the security controls available in the office, workers may fall victim much easier.

TERRANOVA SECURITY