FORTRA

Terranova Security®

Co-présenté par Microsoft

Cybermenaces courantes pour les télétravailleurs

Que vous travailliez à domicile, dans un café, dans la salle de conférence d'un hôtel ou dans un autre lieu éloigné, les cybermenaces peuvent provenir de sources et d'endroits inattendus. Qu'il s'agisse de réseaux non sécurisés ou d'escroqueries visant spécifiquement les télét availleurs qui ne sont peut-être pas encore habitués à leur nouvelle vie, il est essentiel de comprendre comment les cybercriminels peuvent cibler les personnes qui travaillent à l'extérieur du bureau principal.

Les cibles de cyberattaques que les télétravailleurs doivent connaître

01 CONNEXIONS INTERNET NON SÉCURISÉES

Les réseaux Internet non sécurisés, comme un réseau Wi-Fi ouvert dans un lieu public, sont des points d'accès qui ne comportent pas de fonctions de sécurité comme un mot de passe ou des authentifiants. Cette absence de protection essentielle peut rendre toute donnée circulant sur un réseau non sécurisé susceptible d'être volée ou corrompue.

02 ROUTEURS WI-FI DOMESTIQUES

Le fait qu'un réseau Wi-Fi, comme celui de votre maison, ait un mot de passe ne signifie pas que vous êtes automatiquement protégé contre toutes les cybermenaces. Les pirates peuvent cibler les routeurs Wi-Fi en fonction du modèle et du fournisseur d'accès à Internet, ce qui peut exposer les données que les utilisateurs croient sécurisées alors qu'ils travaillent à la maison.

03 MOTS DE PASSE FAIBLES OU RÉUTILISÉS

Les télétravailleurs qui utilisent ou réutilisent des mots de passe courants ou faibles sur diverses plateformes peuvent mettre leurs données confidentielle dans le collimateur d'un cybercriminel. Il suffi d'un seul mot de passe compromis pour que l'identité d'une personne soit usurpée, que son compte soit verrouillé ou que des informations personnelles ou organisationnelles importantes soient exposées.

04 APPÂT OU VOL PHYSIQUE

On parle d'appât lorsqu'une victime est incitée à divulguer des données confidentielles, comme des identifiants de connexion, en échange d'un article ou d'un bien, comme de la musique ou un film gratuits. Cependant, l'appât au moyen d'objets physiques, tels qu'un téléphone ou une clé USB laissés délibérément dans un lieu public fréquenté par des télétravailleurs, peut également servir à voler des données et mener d'autres activités malveillantes.

05 ÉMOTIONS LIÉES À LA NOUVELLE ROUTINE DE TÉLÉTRAVAIL

Les nouveaux télétravailleurs ou les employés qui s'installent dans une routine de travail hybride peuvent être plus sensibles aux escroqueries qui ciblent spécifiquement les personnes travaillant en dehors d'un environnement de bureau. Les cybercriminels peuvent exploiter l'anxiété ou les frustrations liées au travail à distance pour accéder à l'appareil d'un utilisateur et l'inciter à divulguer des informations sensibles.

Qui peut être visé par ces cyberattaques?

Toute personne travaillant à distance ou toute organisation employant une main-d'œuvre principalement distribuée peut être ciblée. Les pirates ont une nouvelle cible de prédilection : le télétravailleur. Les cybercriminels profitent du vi age du télétravail pour cibler les organisations et leurs employés les plus vulnérables. Sans les contrôles de sécurité habituellement effectués au bureau, les travailleurs peuvent être plus facilement victimes.