TERRANOVA SECURITY

TERRANOVASECURITY.COM

5 FAÇONS POUR LES PIRATES INFORMATIQUES DE CIBLER LES ÉTUDIANTS

Nous assistons actuellement à une généralisation de l'apprentissage à distance et de l'intégration de la technologie à l'enseignement postsecondaire. Cette situation a mis en lumière le besoin d'approfondir notre compréhension des façons dont les pirates informatiques peuvent cibler les étudiants et dérober leurs informations sensibles. Ce ne sont pas uniquement les comptes en ligne qui doivent être protégés. Les étudiants doivent également connaître les façons de sécuriser leurs appareils physiques.

Exemples de façons pour les pirates de cibler les étudiants

01 Messages d'hameçonnage

Les cybercriminels ciblent les individus avec des courriels, des messages textes et des messages vocaux. Ces messages utilisent un ton urgent ou menaçant pour encourager le destinataire à passer rapidement à l'action. Il peut s'agir par exemple de cliquer sur un lien ou de partager des identifiants dans un formulaire Web. Le pirate peut également construire son message de façon à ce qu'il semble provenir d'une source sûre, comme un professeur, un administrateur ou un ami.

02 Courriel avec des pièces jointes ou des liens

Pendant une cyberattaque, un moyen populaire de convaincre les utilisateurs d'installer un rançongiciel ou un maliciel sur leurs appareils est de les encourager à cliquer sur une pièce jointe ou un lien alléchant, ou de démarrer un téléchargement automatique. Une fois installés, ces types de logiciels malveillants peuvent compromettre vos appareils, d'autres appareils connectés au réseau et toutes les données stockées ou partagées entre eux.

03 Vol de biens physiques

Les cybercriminels dérobent également des données sensibles via le vol de biens physiques, comme des ordinateurs portables, des appareils mobiles, y compris des téléphones intelligents ou des tablettes, ou des supports de stockage amovibles, y compris des clés USB ou des disques durs. Le vol de données peut aussi survenir si un appareil est laissé sans surveillance dans un lieu public, comme un café, ou si des documents contenant des données sensibles sont exposés aux regards indiscrets.

04 Mots de passe faibles

Si vos mots de passe sont faibles, ou que vous n'en avez pas, un cybercriminel peut en profiter pour s'introduire dans n'importe lequel de vos comptes en ligne. Une fois qu'il possède vos mots de passe, il peut compromettre vos données sensibles, changer vos mots de passe pour vous bloquer l'accès à votre compte et commettre d'autres actes malveillants. Si un mot de passe faible est utilisé pour plusieurs applications, celles-ci peuvent toutes être compromises par une seule cyberattaque.

05 Logiciel de visioconférence

Avec l'essor de l'apprentissage à distance et des classes virtuelles, les applications comme Zoom, Microsoft Teams et d'autres plateformes de visioconférences sont de plus en plus ciblées par les cybercriminels. Si les protocoles de sécurité appropriés ne sont pas mis en place, les pirates peuvent facilement obtenir les liens des réunions, joindre des séances virtuelles, écouter des conversations, interrompre des appels ou vous attirer dans une fausse séance de visioconférence.

QUI PEUT ÊTRE LA CIBLE DE CES CYBERATTAQUES?

Tous les étudiants, peu importe leur emplacement, leur établissement d'enseignement ou leur mode de vie, peuvent être la cible d'une cyberattaque.

Les pirates utilisent les techniques d'ingénierie sociale pour vous amener à divulguer des informations sensibles ou exploiter des failles technologiques. Beaucoup de variables différentes sont en jeu dans un environnement d'apprentissage en ligne. Les étudiants, qui doivent déjà jongler avec le stress lié aux examens ou aux devoirs, peuvent être tentés d'omettre la formation sur la cybersécurité, ouvrant ainsi la porte à l'exposition de données sensibles.

TERRANOVA SECURITY