FORTRA

Terranova Security®

5 façons pour les pirates informatiques de cibler les étudiants

Aujourd'hui, l'apprentissage à distance et de l'intégration de la technologie font partie intégrante de 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 personnelles. Ce ne sont pas uniquement les comptes en ligne qui doivent être protégés. Les étudiants doivent également apprendre à mieux 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

Une des techniques les plus utilisées par les cybercriminels pour convaincre leurs victimes d'installer un rançongiciel ou un maliciel sur leurs appareils est de les encourager à cliquer sur une pièce jointe ou un lien retenant l'attention afin de démarrer un téléchargement automatique. Une fois installés, ces types de logiciels malveillants peuvent compromettre les appareils de la victime, 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, des tablettes, ou des supports de stockage amovibles comme 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 en possession de 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 de 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 et leur établissement d'enseignement, peuvent être la cible d'une cyberattaque. Les pirates utilisent des techniques d'ingénierie sociale pour vous amener à divulguer des informations sensibles ou exploiter des failles technologiques. Beaucoup de variables différentes sont à prendre en compte pour assurer la sécurité de tous dans un environnement d'apprentissage en ligne. Les étudiants ne doivent pas négliger la formation sur la cybersécurité, sous peine d'être exposés ou d'exposer son établissement à la perte ou au vol de données sensibles.