Types de cyber menaces

Vol d'identité

Un type de fraude qui survient lorsqu'une personne obtient et utilise les identifiants d'une autre personne sans sa permission. Il peut s'agir par exemple d'un vol de numéro de carte de crédit ou d'informations sur le compte bancaire d'une personne.

Logiciel malveillant (ou malware)

Logiciel malveillant qui peut infecter votre ordinateur. Il peut être utilisé à des fins d'enrichissement personnel ou pour causer des dommages à l'ordinateur.

Rançongiciel (ou ransomware)

Type de logiciel malveillant qui restreint l'accès à un système informatique ou à un réseau jusqu'au paiement d'une rançon. Il se présente généralement sous la forme d'une pièce jointe à un email et crée un écran de verrouillage avec des instructions que l'utilisateur doit suivre.

Violation de données

Lorsqu'une personne non autorisée accède à des informations personnelles ou confidentielles sensibles. La violation des données peut entraîner de graves conséquences pour une entreprise, telles que le vol d'identité et des pertes financières.

Cheval de troie

Type de logiciel malveillant souvent utilisé pour accéder aux données d'un ordinateur ou d'un réseau. Ils exploitent généralement les failles de sécurité pour pénétrer dans le système informatique.

Logiciel espion (ou spyware)

Logiciel installé à l'insu ou sans l'accord de l'utilisateur. Il peut être installé à distance et possède des fonctions qui lui permettent de collecter des données sensibles sur un ordinateur.

Le hameçonnage (ou phishing) et le harponnage (ou spear-phishing)

Cette pratique consiste à envoyer un email qui semble provenir d'une source légitime afin de voler des informations confidentielles. Le harponnage (spear-phishing) est une forme plus avancée qui cible des individus spécifiques. Les harponneurs utilisent des informations personnelles sur leurs victimes pour rendre leurs emails plus crédibles.

Déni de service

Empêche les utilisateurs légitimes d'accéder ou d'utiliser un ordinateur ou un réseau. La personne qui commet l'attaque utilise les ressources de son propre ordinateur ou réseau pour inonder le système de la victime d'un trafic plus important que ce qu'il peut supporter, généralement dans le but de le rendre inutilisable.