

Saint Valentin : Attention aux arnaques en ligne

Internet

Post   par : JulieM

Publi  e le : 8/2/2023 13:00:00

Pourquoi les escroqueries autour de l'amour et des relations sentimentales sont-elles populaires ?

"Les escroqueries    caract  re romantique sont populaires parce qu'elles touchent des cordes sensibles. Les gens sont moins m  fiants lorsqu'il s'agit d'amour et de relations, et baissent souvent leur garde alors qu'ils seraient beaucoup plus prudents dans une autre situation.

Ces attaques, qui rel  vent g  n  ralement du domaine de l'ing  nierie sociale (c'est    dire qu'elles visent    d  cl  ncher une action pr  cise de la part de son destinataire), mettent l'accent sur la vuln  rabilit   en exer  ant une pression sur une personne pour lui donner un sentiment d'urgence ou en la d  tournant de toute pens  e rationnelle.

Et la collecte d'informations pour identifier et exploiter la cible vis  e est plus facile que jamais pour les cybercriminels. Les applications de rencontres et les profils des m  dias sociaux regorgent de d  tails intimes sur la vie d'une personne.

Les internautes publient sans sans rendre compte un grand nombre de donn  es tr  s int  ressantes pour les cybercriminels : le statut d'une relation, la profession, les loisirs, les photos personnelles et parfois les num  ros de t  l  phone ou les adresses.

Ces informations permettent aux cybercriminels, soit de cr  er manuellement de faux profils attrayants et d'entrer en contact avec des utilisateurs cibles, soit de cr  er des robots qui se chargeront de l'ensemble du cycle d'attaque    leur place.

Une fois qu'un attaquant a trouv   une victime potentielle, il peut tenter d'obtenir des informations personnelles par le biais d'une usurpation d'identit   ou des gains mon  taires par le biais du chantage. Dans certains cas, il peut m  me partager des liens malveillants pour lancer toute une s  rie d'autres attaques."

Quelles sont les attaques les plus courantes ?

"Les cybercriminels optent pour ce qui fonctionne. Les escroqueries romantiques ne font pas exception    la r  gle et s'appuient g  n  ralement sur des techniques   prouv  es de phishing et de spear phishing.

Elles visent    duper les victimes pour qu'elles r  v  lent des informations personnelles telles que le nom de leur animal de compagnie, qui est une question de s  curit   fr  quente sur les sites web, et des num  ros de t  l  phone qui permettent de suivre et de localiser plus facilement une personne.

Cependant, les possibilit  s d'extorsion, de chantage et d'autres fraudes sont bien plus insidieuses lorsqu'il s'agit d'une relation amoureuse, impliquant souvent des images ou des vid  os explicites, ainsi que des demandes de fonds importants pour des d  placements et des d  penses en vue d'une rencontre qui n'aura jamais lieu, etc."

Quels sont les signes d'une   ventuelle de ce type d'escroquerie ?

"Si quelque chose vous semble anormal, c'est probablement le cas. Une diction, une orthographe et une structure de phrase étranges devraient immédiatement vous alerter et vous faire penser que vous avez affaire à quelque chose de malveillant, comme un robot ou un autre programme d'Intelligence Artificielle.

Si une personne est trop directe ou trop personnelle sans aucune interaction préalable, posez-lui une question personnelle assez complexe. Cela permettra de briser les tentatives d'un robot de suivre un script ou obligera l'escroc à essayer de ramener la conversation vers son objectif.

Méfiez-vous également des demandes d'aide ou d'argent qui sortent de nulle part. Les demandes de fonds par des moyens inhabituels, tels que les demandes multiples de cartes-cadeaux ou les transferts de bitcoins, doivent susciter l'inquiétude et donner lieu à une réflexion plus approfondie.

En ce qui concerne ce type d'escroqueries, soyez conscient que les applications de rencontre regorgent de bots et d'escrocs, ce qui fait que vous avez de fortes chances d'être confronté à l'un ou l'autre.

Si vous pensez être une cible, assurez-vous de "blacklister" cette "personne" dès que possible. Et si vous voulez contribuer à l'amélioration de ces plateformes, faites un rapport et laissez l'équipe de modération de l'application prendre le relais."