4 tips on how to avoid getting swindled in dating scams

During the month of love, cybersecurity experts are urging people to exercise caution when they are approached on dating websites or apps.

Image source: Castorly Stock from Pexels

According to Duane Nicol, cybersecurity expert at Mimecast, reports of romance fraud have soared during the pandemic, with some fraudsters going as far as posing as Nicolas Cage to trick their victims into handing over cash.

"Cybercrooks that prey on vulnerable people online are nothing new. However, with the impact of successive lockdowns on people's mental state and the general uptick in cybercrime activity since the start of the pandemic, these types of scams have grown in popularity, with often devastating results for the victims."

The dark side of romance

In late 2021, eight Nigerian men appeared in court in South Africa after a massive international operation where the FBI, US Secret Service and Interpol helped the Hawks arrest them in connection with dating scams, where they defrauded a number of victims out of a combined R100-million. All the women who fell victim to the scam believed they were in serious romantic relationships after meeting their supposed partners online.

"One of the most effective tactics used by dating scam fraudsters is social engineering, which utilises a potential victim's personal information - often publicly available on popular social media sites - to psychologically manipulate them into sharing sensitive personal and financial information, or even cash," explains Nicol. "By the time the victims become aware of the scam, the fraudsters have often made away with their money and disappeared without a trace."

Social engineering recently gained greater public awareness following the release of Netflix documentary *The Tinder Swindler*, which detailed how one scamster tricked several women in Europe into taking out loans and sending him nearly $10-million - or R156-million - before he disappeared.

What is shaping culture? Dating online

Brett Rogers 3 Aug 2020

Dating scams pose risk to employers too

According to Nicol, dating scams could pose a threat not only to the intended victim but to their friends, colleagues and even workplace. "A fraudster could manipulate their victim to divulge sensitive information about their employer that can later be used to commit further fraud. For example, if the victim works at a bank, the fraudster could try to gain inside information about certain security processes and use this knowledge to exploit vulnerabilities."

One of the most effective ways for organisations to protect themselves against cyber risks - including social engineering - is to conduct regular cybersecurity awareness training. "Empowering employees with tools and knowledge to help them identify and avoid potential cyber threats can protect employees and the broader organisation," explains Nicol. "Considering the mental toll that the pandemic has taken on professionals, this additional support is vital as it builds greater resilience among an organisation's last line of defence: their employees."

Tips to keep safe on dating apps

To protect against dating scam fraudsters, Nicol provides tips to help users stay safe:

- **Look out for warning signs:** “There are some telltale signs to look out for when determining whether the person on the other end of the dating app is who they say they are. Fraudsters will often be unable to meet in person or keep postponing an in-person meeting. They can never video call or, when they do, they’re not in the picture. There is often also some major problem in their lives – a sick child, faceless enemies pursuing them, a dying relative – and they urgently need money. Once you give them some, though, there is the inevitable request for more.”

- **Don’t use work devices for personal activities:** “Avoid using your work devices for personal activities, as it increases the risk of clicking on infected links and exposing your company to cyberattack. Any use of personal webmail or other personal account log-ins on a work device will increase the potential that you or your employer become compromised.”

- **Keep your wallet shut:** “Never transfer money to someone you haven’t met face-to-face, even if you have been communicating for months. Fraudsters often use photos of people wearing smart business clothes or uniforms to instil a sense of trust, so it’s important you first verify that the person is being honest.”

- **Get help:** “If you end up in a situation where you think you’ve fallen victim to a crime, contact the police immediately. There may be some feelings of shame associated with being scammed but remember that these fraudsters excel at tricking people, and you are far from the only victim.”