Deloitte.

Technology and Fraud

How technology has changed fraud and what people can do to protect themselves

In the past 10 years we have seen increasing levels of sophistication in fraud schemes and a significant rise in the number of cyber-criminal groups and organisations targeting both companies and individuals with such schemes.

Traditional fraud, focussed on monetary assets, continues to exist but the exponential growth in the amount of data held by companies, facilitated and created by technology, is now a target for fraudsters. On the dark web, private health data typically sells for 10 times more than other personal data.

As our lives and finances move ever more online, so too does fraud.

The introduction of chip and pin on credit cards saw a significant reduction in credit card fraud but this has seen fraudsters move online with a rise in online payments fraud.

Phishing continues to be one of the most common and effective methods for fraudsters to target victims. Estimates suggest that over 90% of cyberattacks start with a phishing email, tricking users into handing over information. While many phishing emails use generic wording, some fraudsters are using personal information about you (typically sourced from social media) to add legitimacy to their requests. This tactic is known as "spear fishing".

Advances in technology have made it easier and cheaper than ever for fraudsters to dupe victims. For example, professional-looking websites or near replicas of legitimate websites can be pulled together in minutes with little or no technical knowledge and at very little cost to lend credibility to fraud schemes.

Advances in communications technology have created messaging and chat appsthat enable fraudsters to collude in more covert ways. Thankfully, advances in discovery technology mean that conversations held using such applications, can be easily and effectively analysed using appropriate tools, should an investigation prove necessary.

AI – Friend or Foe?

Developments in Artificial Intelligence ("AI") are likely to pave the way for future frauds. Given a sample of a target's voice, AI methods can now generate speech in their voice and this can be overlaid on synthesised video of them speaking with very convincing results. This could then be used to commit frauds like those described above.

Of course AI can be a source for good. AI-enabled data analytics can now identify and stop transactions before they are processed.

What can you do to protect yourself?

These tips may seem self-evident but trust me they will help in protecting you!

1. Stay fraud aware – Use the many resources available online to ensure you know about the latest fraud scams and how you can avoid them
2. Think before you share – The information you share online can be dangerous in the wrong hands. Do you REALLY need to share it? If not, DON'T!
3. Be sceptical – If a situation seems odd or an offer seems too good to be true, it probably is. Trust your instincts and follow them making whatever enquiries you need to, to ensure you don't fall fowl of fraudsters.

Contact

Shane Flanagan
Forensic
Dublin
D: +353 (0) 1 417 2433
shflanagan@deloitte.ie