Social Engineers

How Yesterday's Con Artists Have Become Today's Online Fraudsters

By Mark Johnson

Mark is a former military intelligence officer, drug enforcement agent, and global head of network fraud and security, now engaged by QA Consulting, the City of London Police, the National Police Chiefs' Council, CIFAS, the International Compliance Association, and MIS Training Institute as a cyber-crime and open source investigations (OSINT) trainer and consultant. He can be contacted at markj@trmg.biz.

Have you ever been conned? Tricked into investing in a fake property scheme? Made to believe that you're in line for a specific prize when a hundred thousand other people share the same fantasy? Have you been duped by a partner, love bombed by someone you had only just met, or ripped off by your child? If the answer to any of these questions is yes, then you have already been the target of malicious social engineering.

Malicious social engineering has evolved beyond the simple con. As organisations respond to the threat of cyber-crime by introducing sophisticated controls, cyber-criminals have increasingly focused on human beings as targets. After all, we can update our software with relative ease, but updating people is a much tougher challenge; just push that romance button, and all those hours of security awareness training can suddenly become worthless.

Consequently, most cyber-attacks begin with a social engineering phase: gathering intelligence, tricking users into giving up passwords, or persuading people into clicking links and giving up personal or financial data or downloading spyware and ransomware. If attackers realise that this approach isn't viable on corporate systems, personal and Internet of Things devices, from laptops and mobile phones to smart TVs and webcams, are often equally valuable targets because they can hold personal data or passwords and might be taken into work and connected to the business network. Often, they can be added to the attacker's own network of hacked devices within a so-called "botnet," a network of infected bots.

Malicious social engineering has evolved beyond the simple con. As organisations respond to the threat of cyber-crime by introducing sophisticated controls, cyber-criminals have increasingly focused on human beings as targets. After all, we can update our software with relative ease, but updating people is a much tougher challenge.

Social engineering threats, therefore, are near the top of the list of threats that loss prevention and security teams need to understand and prepare for. So let's explore a few examples of modern social engineering in action and discuss the responses these require.

The Case of the Vengeful Hairdresser

Last year I was asked by a law enforcement client to examine a set of social media profiles that had featured in an online harassment campaign. There were forty-two profiles in total, and my initial instinct was that they belonged to forty-two different people; each was unique with different names, photos, and activities.

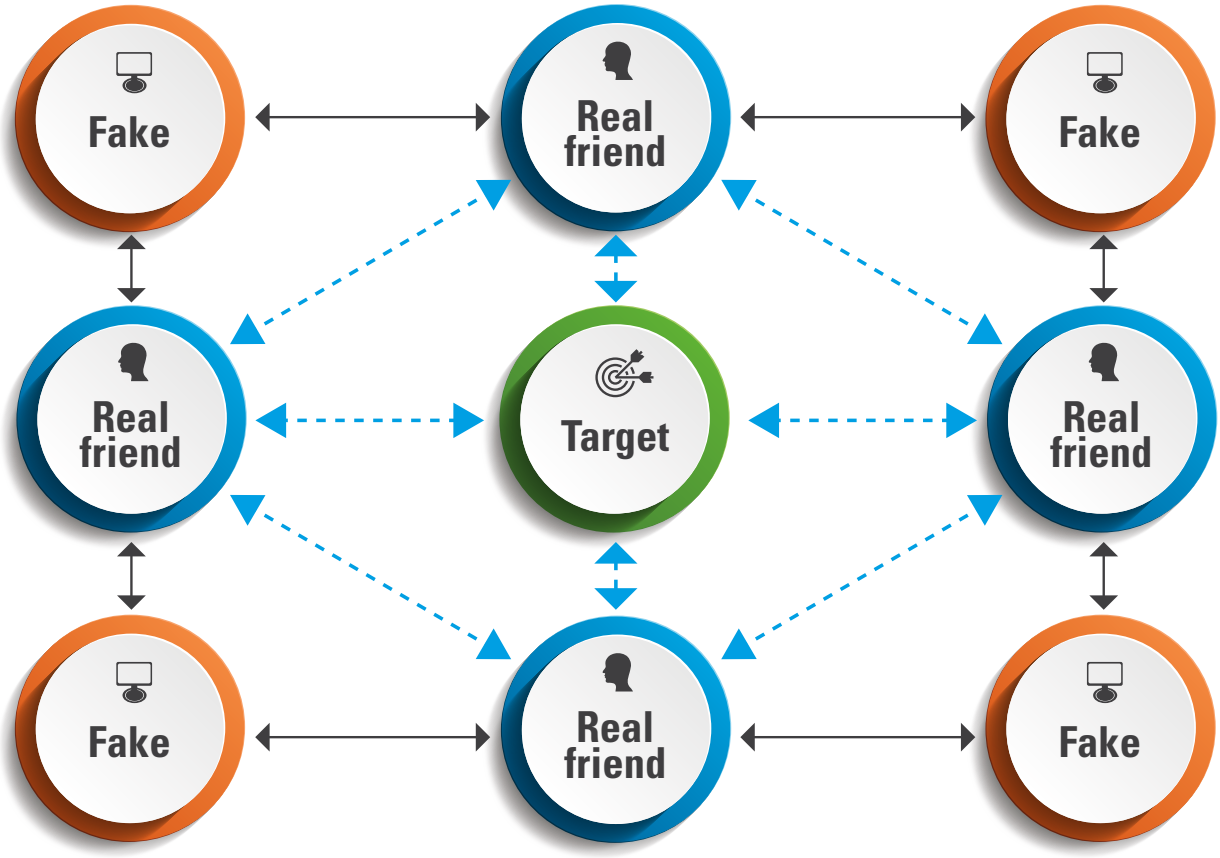
More in-depth analysis revealed that all forty-two profiles were fakes. They had been set up and were being used by just one angry young woman, a nineteen-year-old hairdresser. She had been dumped by her boyfriend and was targeting his new partner who had just given birth to his child.

Rather than approaching her target directly, the hairdresser busily made friends with the target's own friend network. The forty-two fakes each had over one hundred friends, all of whom were friends of girl number two. She surrounded her target with a vast web of fake links and associations, friends of friends and then friends of their friends, a virtual spider's web of fake connections.

This was only possible because, like most users, the new girlfriend had left her social media profile settings at the default level; anyone could see her profile, timeline, posts, and friends list. Anyone could therefore send friend requests to her friends and create fake profiles that were of a similar type, in terms of demographic, interests, and apparent lifestyle.

The hairdresser had ensured that her forty-two fake profiles would be accepted by the unsuspecting friend network of her target. This was classic social engineering stuff and very professionally executed. I admit that I was hugely impressed. The effort she had invested was hard to imagine, as was her level of fury and her desire for revenge.

With her intended victim surrounded, the vengeful hairdresser now carried out her attack. She created an in-memoriam tribute page dedicated to the newborn child of the new girlfriend and bearing the child's photo, although there was nothing wrong with the child in reality. Nevertheless, the mother now received a tsunami of condolence messages, coming not only from her friends, but from the friends of her friends (including the hairdresser's forty-two fake profiles), and from hundreds of *their* friends. The emotional impact of this virtual death threat can only be imagined.



Understanding the "Cyberpath"

The example of the vengeful hairdresser is illustrative of the obsessive, merciless approach to online social engineering that is a hallmark of digital criminals. I have described this class of actor as "cyberpaths," online sociopaths who exclusively use digital channels. Today there are millions of such actors, and the very nature of the Internet fosters their development because it puts them anonymously in touch with victims at a distance.

Urban Dictionary now defines a cyberpath as "an individual with a pathological disorder who has access to the Internet and uses the Internet as a medium for acting out his or her pathology." Some of the key characteristics I assign to the typical cyberpath include:

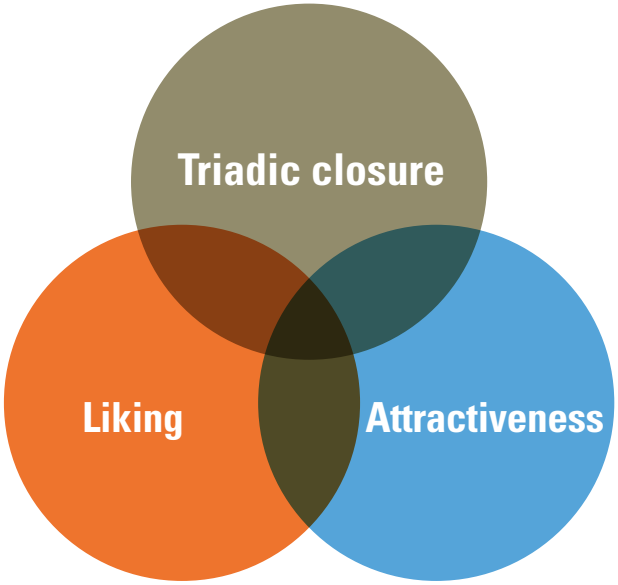
- Lack of remorse.
- Lack of conscience.
- Obsessive behaviour.
- Strong social engineering abilities.
- Some degree of technical or online skill.
- Engagement in fraud, stalking, grooming, harassment, or seeking revenge for perceived wrongs.

Many internet trolls are clearly cyberpaths, according to the above definitions. When a cyberpath adds a financial or ideological dimension to their list of motivations, they morph into an online fraudster or unethical hacker, but the underlying character traits remain the same.

The Social Engineering Magic Formula

The cyberpathic hairdresser had, without any training in the domain, re-invented a simple but powerful social engineering formula with three core elements: triadic closure, attractiveness, and liking.

When used in a social media context, "triadic closure" refers to the act of connecting with friends of the target before approaching the actual target. The common result of this is that



when a target receives a friend invite from the fraudster, they will see that they already have friends in common, which may induce them to accept the request without investigating it further.

"Attractiveness" means that social engineers will do their best to make their profile or offering appealing to the victim. They learn what this appeal might be by studying the target's online life. The default settings on most social sites, which are generally insecure, make the act of discovery very easy to carry out. We are required to opt-in to security, rather than opting out.

Use of "like" buttons, following, commenting, and reposting, in combination with triadic closure and attractiveness, can further enhance the possibility that a victim will entertain invitations or messages from the attacker; they see someone appealing, who has friends in common and who finds their online posts interesting.

It takes a very well-trained member of staff to see through engineering of this nature.

Vulnerable Insiders

Successful social engineers don't employ these methods at random. They first search for vulnerable targets and then structure their approach. A degree of amateur psychology is often involved in these assessments.

There are a myriad of ways to achieve a result like this, but common ploys include:

- Google searching the target's email address to identify social accounts and handles (usernames) they might have online.
- Google searching any online handles found. This can bring up supposedly anonymous posts on a range of sites that reveal the personal interests and opinions of the target.
- Using Google to reverse search images of the subject, such as profile pictures on social pages that have not been locked down. This will uncover any other online sites on which the same picture has been used, providing further clues about the target's personality.
- Armed with photos of the target, fraudsters can loiter near their place of work and swipe through dating app profiles, with the search settings adjusted to one kilometre and matching the age range of the target. Dating profiles often reveal intimate details or allow an attacker to engage in romantic or salacious discussions. Psychological pressure can then be used to influence a vulnerable target.

The Role of the Deep Web

In addition to the vast quantities of personal information freely available in the Surface Web, huge repositories of sensitive data are held in the Deep Web. This comprises academic and public sector sites, such as Companies House, that are not indexed by search engines like Google, but which anyone can access.

With 75 per cent of small and medium UK enterprises having their registered address at the home of the founder, the scope for abuse by cyber-criminals is very significant. Was it really our intention that anyone on the planet could see this information without needing to provide any justification whatsoever?

Darknet Markets

The encrypted and anonymous domain that is the Darknet serves two critical purposes of value to online criminals. It is a place in which the tools for committing crimes can be easily obtained, as well as being a marketplace for selling stolen data. Some experts have calculated that up to 50 per cent of the sites hidden in the Darknet, which is largely funded by the US government via the Tor Project, are involved in activities classed as criminal under UK law. These are often described as "Crime-as-a-Service" offerings, or CaaS.

It's Partly about Settings

Many of the social engineering ploys we see in the wild exploit weaknesses in social media sites, dating apps, and the indexes compiled by the leading search engines. Most such sites have thus far failed to introduce the most fundamental security settings. If you look up a list of the top ten online security controls recommended by the leading providers of such guidance, and then assess the default settings provided by the top social media providers, you will likely see that all such sites fail to meet the most basic thresholds.

Corporate liability for weak security design must become part of the mix. Suppliers who provide insecure products or services should be banned from the market, and the directors of those firms must be held to account. The principles of security by design and default need rigorous enforcement. The days of the digital Wild West must now end.

Rather than opting out of security online, we have to opt in. The most important steps that every user should take and that every employer should audit include:

- Never use profile pictures that are online anywhere else.
- Never provide more than the most basic personal data to any site; an email address and password are generally all that you need to surrender.
- Never post your employer's identity on personal sites (such as Facebook or Instagram).
- Never post your personal details on business sites like LinkedIn.
- Never reveal your phone number, work email address, or personal email address. Users should contact you via the site.
- Carefully examine friend requests to check for fakes. If a stranger has friends in common, ask those friends how they know the person before you click accept.
- Look at and use the available security settings. Do you really want everyone on the planet to see your full profile?

For a more detailed breakdown of the security settings available in many of the major sites, you can access our free *Secure Online Book* in the Knowledge Zone at trmg.biz. We do not capture your details, and no email contact will follow.

A Digital Wild West

When we add the ease with which fake domains can be registered, the role of "paste sites" such as Pastebin.com, and the facilitation by Google of searches for Fullz lists, Dorks lists, and even email address lists in Excel format, it is clear that we are operating in the digital Wild West. Solutions are urgently needed.

It's Time for EU GDPR II

The EU's General Data Protection Regulation (GDPR) represented a significant step forwards in assigning responsibilities and defining penalties. What it lacked, and what GDPR II needs to urgently address, is security benchmarking. We need to spell out what good information security looks like in practice.

If, for example, Apple releases a phone that lacks effective user access and authentication controls, then Apple needs to be held accountable for the resulting data breaches and fraud incidents. Corporate liability for weak security design must become part of the mix. Suppliers who provide insecure products or services should be banned from the market, and the directors of those firms must be held to account.

The principles of security by design and default need rigorous enforcement. The days of the digital Wild West must now end. ■