Security & Privacy, 2012, 10(1): pp.28-36.
7. Gates, WH. Keynote presentation, RSA conference, 2004.
8. Bonneau, J; Herley, C; Van Oorschot, PC; Stajano F. 'The quest to replace passwords: A framework for comparative evaluation of web authentication schemes'. In Proceedings of the 2012 IEEE Symposium on Security and Privacy, ser. SP '12, 2012: pp.553–567.
9. Akhtar, Z; Micheloni, C; Foresti LG. 'Biometric liveness detection: Challenges and research opportunities' IEEE Security & Privacy, 2015. 13(5): pp.63-72.
10. O'Gorman L. 'Comparing passwords, tokens and biometrics for user authentication'. Proc. IEEE, 2003. 91(12): pp.2019–2040.

Bad behaviour: exploiting human weaknesses

Steve Mansfield-Devine

Steve Mansfield-Devine, editor, *Computer Fraud & Security*

It's all too easy to see computer security as a technology issue – and one that can be fixed by throwing more technology at the problem. And yet the key element in many attacks is human frailty. Various malicious actors – from fake Nigerian princes to state-backed cyber-warriors – continue to use tried and tested social engineering techniques to convince people to do things that are not in their best interest. As Markus Jakobsson, chief scientist at email specialist Agari, explains in this interview, the technology and techniques involved in online scams have evolved – and so have our responses – but the underlying flaw remains human nature itself.

Frauds committed via email are among the oldest forms of cybercrime. Many of them evolved from scams perpetrated via postal mail and fax – they simply grabbed on to the sudden uptake of email among the general population as a way of scaling their operations. Typical frauds include: the fee-forwarding scams most commonly associated with Nigerian gangs; romance scams, such as those young, attractive Russian or Ukrainian women who discover a sudden passion for rather average Western men; a wide variety of phishing attacks, which can be aimed at simply harvesting login credentials or can signal the prelude to a much more serious, targeted hacking attack; and so-called 'CEO fraud' – more accurately known as business email compromise (BEC) – in which attackers impersonate senior executives to persuade employees to transfer funds.[1]

In a recent webinar, Jakobsson outlined a taxonomy of attack types used in email-based scams where faked identities are a key element in the crime.[2] For example, phishing emails may purport to come from organisations such as banks, PayPal, Google and so on. BEC scams depend on emails that seem to originate from senior executives, often within the same organisation as the target. To achieve their aims, such emails use a number of methods, including:

- Spoofed domains where the email headers are manipulated to appear to come from the same company as the victim, or from another legitimate organisation.
- Look-alike domains close enough to the genuine domain to pass all but close scrutiny. In his webinar, Jakobsson gave the example of an attacker using the domain acrne.com to imitate acme.com.
- A display name for the email account crafted to look legitimate and perhaps familiar. Most people only look at the name and not at the full email address. On some platforms – particularly mobile ones – the email address might not be displayed.
- Genuine email accounts and domains where the attacker has somehow gained access to the account (perhaps through an earlier phishing attack), or is simply using his own.

We all like to kid ourselves that we can easily spot an imposter. And indeed, if you go back 10 years or so, many scam emails were somewhat obvious. The message would fail to mention the intended victim by name, would contain grammatical and spelling errors or inappropriate language, would lack corporate branding and would generally appear unprofessional.

One area where the attackers have become more sophisticated, says Jakobsson, is through exploiting our expectations. Technology is now an integral part of our private and professional lives and the scams work by exploiting the daily patterns in our use of it.

"When it comes to the trickery, many successful attacks are those that somehow follow the normal workflow of people," he explains. "We know that we have to update passwords every once in a while, whether it's because of some kind of breach, or because somebody is attacking your account, or maybe just the password

Markus Jakobsson, Agari: "Many successful attacks are those that somehow follow the normal workflow of people."

got old enough. So that is one workflow. Similarly, everybody knows that companies receive invoices and those invoices have to be paid. And so that's another workflow that the scammers use. They simply inject invoices into the system, or trick recipients into replacing existing invoices with new invoices."

He adds: "If it looks similar to the normal workflow, you've got the feeling of familiarity. And also, when you're at work and you're asked to do something that supposedly relates to your work, why would you question it? You were hired to do that, why would you create trouble for your colleagues by not doing it? So the attackers make people feel, 'well, even though it's a little bit unusual, I'd better go out of my way, because it's obviously important'."

It seems that most people only need a few convincing details to persuade them that an email is legitimate. Jakobsson explains an experiment he recently ran that demonstrates this.

Overcoming suspicion

Even where you might expect some reticence or suspicion, the corporate environment can work in the attacker's favour. With BEC, for example, the faked message might stress that the funds transfer being urgently demanded is part of an acquisition and therefore dreadfully secret. "You can't talk to others about it, because it's about the acquisition and because of regulation," says Jakobsson. "There are the many ways in which to make people do things and not speak about it."

In the case of CEO fraud, one can easily see how a busy person might be tricked into transferring small amounts to the attackers' accounts. But it's a measure of the power of email scams that the results can be spectacular. In 2015, networking company Ubiquiti Networks was taken for $46.7m when one of its overseas subsidiaries was conned into a series of wire transfers.[3]

"This fraud resulted in transfers of funds aggregating $46.7m held by a company subsidiary incorporated in Hong Kong to other overseas accounts held by third parties," the firm announced at the time. "As soon as the company became aware of this fraudulent activity it initiated contact with its Hong Kong subsidiary's bank and promptly initiated legal proceedings in various foreign jurisdictions. As a result of these efforts, the company has recovered $8.1m of the amounts transferred."

Earlier that year, a US commodities firm, The Scoular, was tricked into wiring $17.2m to a bank in China. And in early 2016, aerospace company FACC fell for a scam that led it to wire €52.8m to fraudsters in several transactions.[4] Some of the money was intercepted at recipient banks, although it was uncertain at the time how easy it would be to recover. The company recorded a €41.9m loss, which meant that, instead of being in profit that year (as it had been the year before) it was in the red to the tune of €23.4m. The CEO, Walter Stephan, was sacked.

Another high-profile example of how attackers have benefitted from putting greater efforts into credibility is the breach of emails belonging to John Podesta, former White House chief of staff and chairman of Hillary Clinton's presidential campaign. Like other related email leaks – most famously from the US Democratic National Committee (DNC) – the source of this attack is still highly contentious, although US intelligence agencies and most security researchers have pointed the finger at Russia.

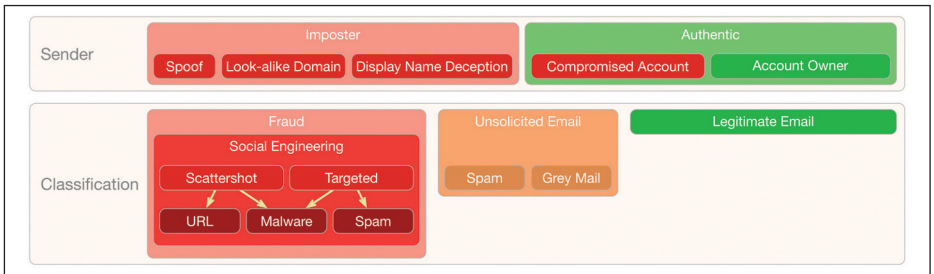
The Podesta breach started with a spear-phishing campaign. Podesta received an email to his Gmail account purportedly coming from Google and saying that there had been an attempt by someone in Ukraine to access the account. This attempt was blocked, the email said, but it went on to advise that Podesta change his password. The email was convincingly formatted using Google's branding and included a large button that linked to a fake login page. The address of the target page was obscured using a URL shortening service.

Because this was delivered to a Gmail account and fraudulently claimed to come from Google, Google's email system had placed it in the spam folder. However, someone had subsequently fished it out of that folder. Podesta queried a number of aides about the email, one of whom, Charles Delavan, wrote back saying: "This is a legitimate email. John needs to change his password immediately."[5] He'd meant to write 'illegitimate'. The end result was Podesta's emails turning up on Wikileaks.

Nigerian princes

There is still one species of scam that appears obviously fraudulent to most of us. This is the so-called 'Nigerian scam' that typically involves someone asking for your help in moving a large amount of money. These messages continue to be poorly constructed and badly spelled. But there is some evidence to suggest that this is a deliberate ploy.[6] These scams usually involve several rounds of interaction between the scammers and their victims and the criminals don't want to waste their time dealing with anyone except the most gullible.

For the most part, though, Jakobsson says the past couple of years have been notable for the increased sophistication



The taxonomy of email-based attacks according to Agari in terms of mechanism used. The frauds that are the subject of this article mostly occupy the red areas.