Report

Hacking the Human Operating System

The role of social engineering within cybersecurity

intel Security

Contents

This report was researched and written by:

Raj Samani, EMEA CTO

Charles McFarland, Senior MTIS Research Engineer

Foreword

Foreword by:

European Cybercrime Centre (EC^3)
Europol

Recent technological developments, complemented by the increased use of and reliance upon the Internet, offer unlimited new opportunities to facilitate our personal and professional lives. Nonetheless, as technology continues to progress, these improvements have also been widely exploited as a tool or infrastructure for committing a wide range of criminal offences. There are numerous types of crime committed daily on the Internet, facilitated by the Internet, or amplified via the Internet that directly target vulnerable devices or trick victims into enabling vulnerable features or exposing user credentials and other sensitive information. The growing Internet penetration and the newly emerging technologies such as the Internet of Things are also changing people's behavior online and create a broader attack surface, new attack vectors, and more points of entry, such as through social engineering techniques, which was also a key finding of Europol's **Internet Organised Crime Threat Assessment (iOCTA) 2014.**

At present, cybercriminals do not necessarily require substantial technical knowledge to achieve their objectives. Some well-known malicious tools are delivered using spear-phishing emails and rely on psychological manipulation to infect victims' computers. The targeted victims are persuaded to open allegedly legitimate and alluring email attachments or to click on a link in the body of the email that appeared to come from trusted sources.

The use of social engineering techniques has become a significant and widespread means of deploying malicious attacks on the Internet to obtain sensitive or classified information from competitors, rivals, and governments, among others. A recent trend in the attacks is their targeted nature: Criminals are using sophisticated and tailored techniques to deploy malware, usually by spear-phishing emails. Another example of such a tactic is whaling, which is aimed at high-profile individuals or members of certain groups of interest for the criminals. While some organized groups may specialize in large-scale cyberattacks and scams by throwing out bait and accepting whichever victims bite, others take advantage of more sophisticated criminal activities and tailored techniques to deploy malware inside a closed organization, government, or financial institution. The adversaries gather intelligence on their targets to learn about their habits and design a tailored attack to manipulate the targets and attain their objectives, such as acquiring sensitive information.

The damaging effect and the financial impact of such human-based attacks have already been brought to the attention of the private and the public sectors, as well as other societal members, by the numerous occurrences of such frauds in recent years. We are witnessing the increased effectiveness of these fraudulent techniques, due to the fact that people are the weakest link in system security and that the opportunity cost of such an attack is often smaller than targeting computers and networks. For example, there is almost no cost for employing social media, spam, and phishing social engineering techniques. We have recently seen variants of phishing, such as bogus websites (pharming), SMS (smishing), and phone or voice over IP (vishing). Moreover, we are observing a growing trend of less technically knowledgeable criminals employing social engineering tactics to fraudulently obtain sensitive information, deploy malware, or coerce a victim into making certain transactions. The Crime-as-a-Service model prevalent in the underground cybercriminal economy significantly facilitates such scams, as the attackers can acquire more sophisticated attack tools or purchase harvested data. Furthermore, due to large-scale company data breaches during 2014,

a large volume of consumer data was exposed; and because such information is a prerequisite for launching spam or phishing attacks, we may see a further proliferation of such attacks in the near future. Despite the limited amount of reliable reporting mechanisms and statistical data on cybercrime, research suggests that the number of businesses that become victims of cyberattacks via phishing and social engineering schemes is on the rise.

Across Europe, we are also observing **an increasing number of victims** of phishing, especially among the elderly who may lack an understanding of the threats posed by the Internet.

From a law enforcement perspective, cross-border social engineering campaigns pose a significant investigative challenge because they affect multiple jurisdictions and are often hard to trace due to advancements in anonymization and obfuscation technologies abused by criminals to conceal their real identities. Nevertheless, European law enforcement has successfully conducted actions against organized crime groups employing such tactics. This is illustrated by an operation led by Belgian and Dutch authorities, and supported by Europol and Eurojust, in May 2014 **in a voice-phishing case** that resulted in 12 arrests and the seizure of cash and important digital evidence. Another example of successful law enforcement activities concerned a national operation against a sophisticated money-mule scam. (Scammers use other people's accounts for fraudulent money transactions and money laundering.) **The action resulted in 18 arrests** of individuals involved in online fraud with bank accounts. In addition to these operations, the development of working relationships between law enforcement and the private sector is instrumental in reducing crimes committed via social engineering and Internet scams. Dutch authorities, for example, have partnered with representatives of the banking sector in the new initiative **Electronic Crimes Task Force** to address and prevent digital crime such as fraud in online banking, financial malware, phishing, etc.

This report from McAfee Labs examines the main threats associated with human-based attacks for information gathering, fraud, or compromising a computer. We hope the report will help you better understand current risks and threats, and forecast trends in the development of criminal activities.

—European Cybercrime Centre (EC^3)

Introduction

In July 2014, more than 1,000 energy companies in North America and Europe were reported to have been compromised by targeted cyberattacks.[1] Compared with other targeted attack campaigns (such as **Operation Troy**, **Operation High Roller**, and **Night Dragon**), this effort appears different in almost every way. However, the one common theme among all of these is social engineering. Whether the target of the attack is a consumer or an employee in a large enterprise, the modus operandi for most cybercriminals is to employ some form of social engineering to coerce the victim into an action that facilitates the infection.

The prevalence of social engineering in many publicly disclosed cyberattacks suggests that there is either an inherent weakness in the ability of victims to distinguish malicious communications or that cybercriminals are using more complex methods to bypass the "human firewall." The truth likely lies somewhere between these two statements but, regardless of the root cause, we can see that the first line of defense is evidently failing. More important, to simply blame users for breaches is not entirely fair. There are many examples of clearly unsafe user behavior; but this report will demonstrate that attackers often bypass the consciousness of their targets and attempt to manipulate victims through subconscious influences.

This report will review the concept of social engineering. We will consider the techniques used in recent cyberattacks, as well as the levers to influence victims, communication channels, and suggested controls to reduce the risks. This report will define the concepts of social engineering and introduce mitigations that go beyond simply suggesting greater awareness as a panacea.

Twitter@Raj_Samani

Twitter@CGMcFarland

Defining Social Engineering

There are many definitions for the term *social engineering*—also known as pre-texting, blagging, and conning—from the overly specific to the very broad. For the purposes of this report, we will focus on the term's key elements, which are often lost in other definitions.

The following definition highlights the key elements of social engineering:

> *The deliberate application of deceitful techniques designed to manipulate someone into divulging information or performing actions that may result in the release of that information.*

During a social engineering interaction, the victim is not aware that his or her actions are harmful. The social engineer exploits the target's innocent instincts, not any criminal instincts. Attackers employ a variety of methods to trick victims into divulging useful information or performing an action such as clicking a link. Social engineering uses subterfuge to get its targets to take an action that, if they were aware of its real purpose, they would not take. Contrast this with direct techniques such as bribery or the threat of violence. Direct techniques of exploitation do not fall within the scope of social engineering.

A social engineering attack can be targeted or opportunistic. Targeted attacks typically focus on a specific individual, whereas opportunistic attacks aim to glean information from anyone in a specific position (such as a helpdesk).

Defining a Social Engineering Attack

Social engineering categories

Social engineering attacks can be divided into two categories: hunting and farming.

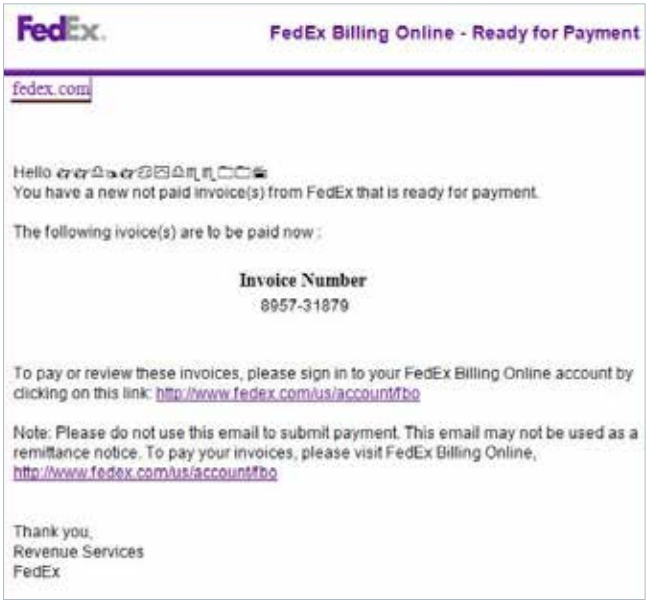
- Hunting aims to extract information using minimal interaction with the target. This approach typically involves a single encounter, with the attacker ending communication once information has been acquired.
- Farming aims to establish a relationship with the target and to "milk" the relationship for information over a longer period.

Over time, the relationship between the target and the social engineer may change. For example, the target may catch on to the attempt and possibly seek remuneration, or the social engineer may attempt to use blackmail, thus moving the interaction from social engineering to traditional criminal behavior.

For more information on detecting spoofed emails claiming origin from FedEx, **click here.**

Examples of hunting

The following example, an email purportedly from FedEx, attempts to coerce the victim into clicking a link.[2] It demonstrates the minimal interaction typical of a hunting attack.



FedEx

FedEx Billing Online - Ready for Payment

fedex.com

Hello [redacted]
You have a new not paid invoice(s) from FedEx that is ready for payment.

The following ivoice(s) are to be paid now :

Invoice Number
8957-31879

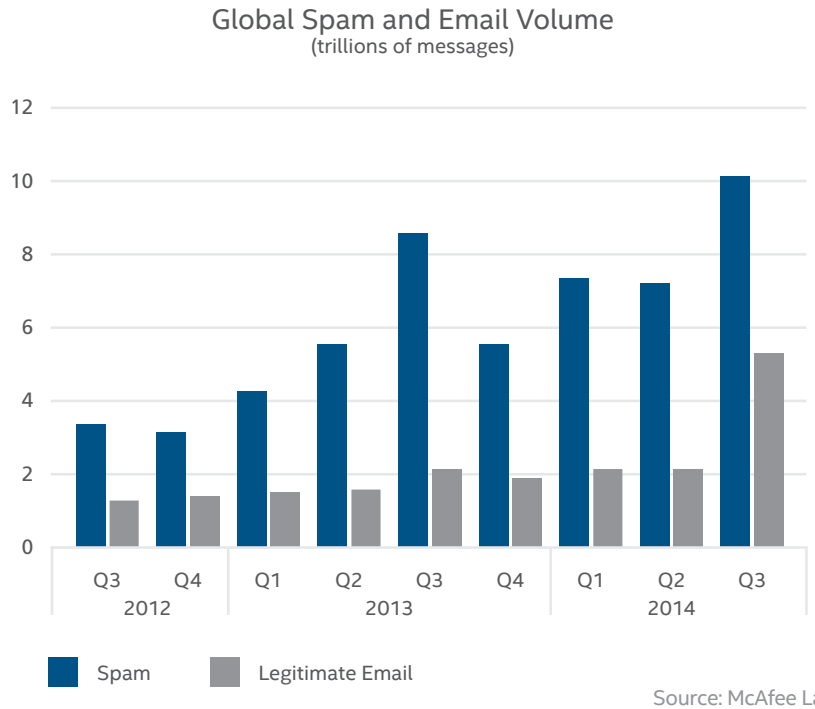
To pay or review these invoices, please sign in to your FedEx Billing Online account by clicking on this link: http://www.fedex.com/us/account/fbo

Note: Please do not use this email to submit payment. This email may not be used as a remittance notice. To pay your invoices, please visit FedEx Billing Online, http://www.fedex.com/us/account/fbo

Thank you,
Revenue Services
FedEx

An example of hunting using a bogus email posing as a FedEx message.

Email is a common vector for social engineering attacks. The recent ***McAfee Labs Threats Report: November 2014*** reports that global spam accounts for approximately two-thirds of global email, as measured by McAfee Labs.

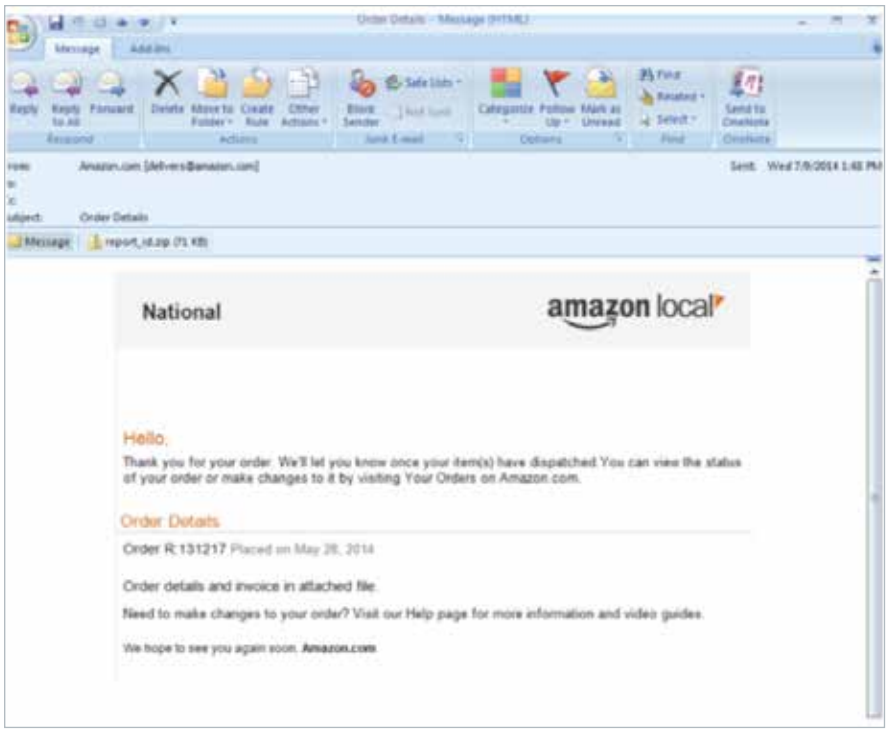


Source: McAfee Labs.

Share this Report

For more information on detecting spoofed emails claiming origin from Amazon, **click here.**

Not every unsolicited message looks to extract data from a victim; however, there is no question that email is a leading vector for social engineering attacks. As we see in the following image, these attempts are predominantly hunting attacks.



This hunting example is an email that appears to be sent by Amazon.com.

The preceding example arrives via email, and tries to coerce the victim into opening the attachment by impersonating a legitimate entity. In this example, it involves minimal interaction with the victim (just one email) with direct communication likely to be terminated after the action is carried out.

An example of farming

The following describes how farming was used in an undercover law enforcement operation in which an agent for the U.S. Federal Bureau of Investigation (FBI) became an administrator for the carder site DarkMarket.

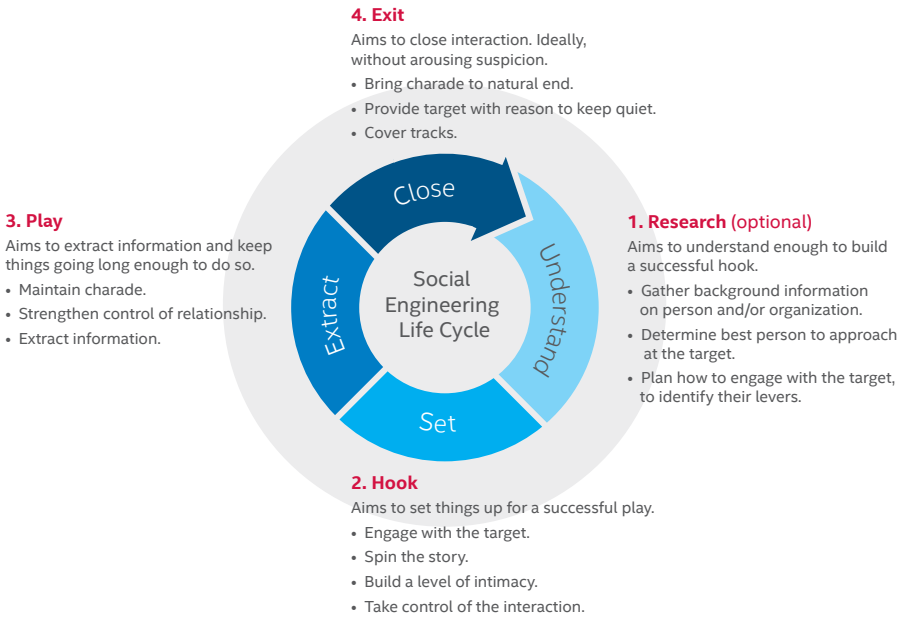
> *"DarkMarket was what's known as a 'carder' site. Like an eBay for criminals, it was where identity thieves could buy and sell stolen credit card numbers, online identities, and the tools to make fake credit cards. In late 2006, [FBI Special Agent] Mularski, who had risen through the ranks using the name Master Splynter, had just been made administrator of the site. Mularski not only had control over the technical data available there, but he had the power to make or break up-and-coming identity thieves by granting them access to the site."*[3]

As this farming example demonstrates, a social engineer needs to create a hook—in this case, the lure of an easy life of crime—in order to develop the foundation for a relationship. Unlike hunting, the interaction between the parties within farming relationships extends over some time. Social engineering farming is not particularly common.

The fundamental difference between hunting and farming is the number of interactions between the social engineer and target. Hunting aims to get information in a single interaction, whereas farming involves ongoing interactions.

Social Engineering Attack Lifecycle

A social engineering attack (whether hunting or farming) typically comprises four phases. Of these four, the first phase (research) is optional because a social engineering attack may involve a chance encounter rather than a targeted attack.



The four phases of a social engineering attack.

Social engineering attempts may be a single action to acquire specific data or part of a much larger campaign to gather multiple bits of related information. For example, the attacker may perform one hunting attack, retrieve the information, and disappear. Or an attacker may perform numerous hunting attacks, and with that collected information initiate a farming attack. Although social engineering attacks are often seen as linear, one attack may lead to another attack, hence the circular lifecycle of the four phases. One example of this circularity was the recent attacks related to **Operation Dragonfly**:

> *"The fact that Dragonfly is gathering information about OPC servers and VPN connections to PLCs might indicate that the final objective is to gain access to the PLCs themselves, which would enable the attackers to change, damage, or disrupt the critical processes run by the targeted organizations."*[4]

Operation Dragonfly used social engineering (hunting in the form of spear phishing), but this could be the precursor for a broader attack to impact the availability of targeted systems. There is no typical duration for each phase. A social engineering attack may consist of one short telephone call, email, or direct message (hunting), or it may span many years with ongoing interactions (farming).

Phase 1: Research

The objective when researching the target is to identify a potential hook or garner information that may assist the play phase, such as learning the jargon of the person or company an attacker is trying to imitate. The social engineer can use a variety of research sources:

- **Online information:** Corporate websites, social networking profiles, web searches, etc.
- **Public documents:** Information from electoral rolls, statutory company returns, etc.
- **Physical interaction:** Socializing with the target, colleagues, or friends.

With the advent of the Internet, much research can be carried out remotely, simply, and at relatively low cost. Sometimes, the social engineer conducting an opportunistic attack may not research the target at all. For example, researching an individual may be unnecessary when conducting a broad phishing campaign, because using a common brand with a generic message can fool enough recipients to incite action.

Phase 2: Hook

A hook aims to set up a successful play. The attacker engages the target and provides a pretext for interaction. Social engineers will attempt to use their influencing skills in the hook phase. Psychologist Robert Cialdini cites six influencing levers, which aim to leverage the subconscious.[5]

These influencing levers are used for many purposes—including sales, cons (trying to extract money from people), and social engineering. Some of the following examples do not target information but demonstrate the use of the influencing lever.

- **Reciprocation:** When people are provided with something, they tend to feel obligated and subsequently repay the favor.

  Example: "An employee receives a call from a person who identifies himself as being from the IT department. The caller explains that some company computers have been infected with a new virus not recognized by the antivirus software that can destroy all files on a computer, and offers to talk the person through some steps to prevent problems. Following this, the caller asks the person to test a software utility that has just been recently upgraded for allowing users to change passwords. The employee is reluctant to refuse, because the caller has just provided help that will supposedly protect the user from a virus. He reciprocates by complying with the caller's request."[6]

  Social networks—for example, LinkedIn—use reciprocation to accumulate endorsements and followers. Recently, a strategy for accruing more Twitter followers through reciprocal following uses the same lever.

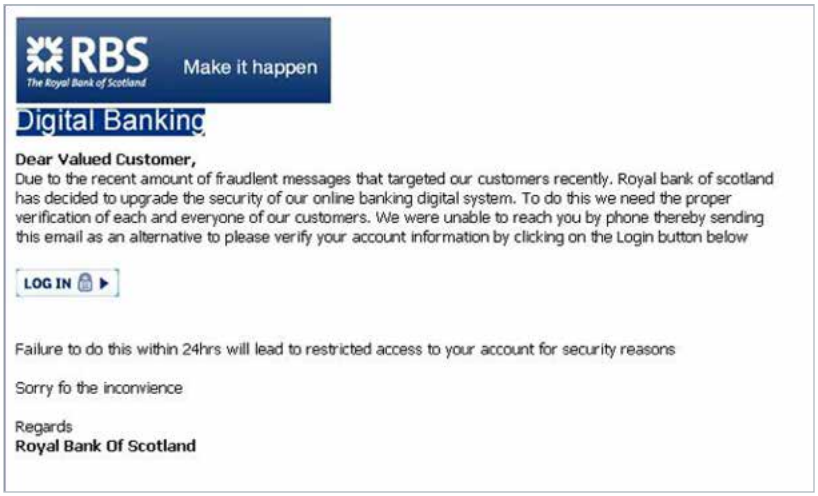
For more information on detecting spoofed emails claiming origin from U.S. Bank, **click here.**

- **Scarcity:** People tend to comply when they believe something is in short supply.

  Example: "[A] 'spoof' email claims to come from U.S. Bank. Email contains bank logos and tells recipient to provide account information through a web link. The recipient is also told that if they don't comply with the instructions, their account will be disabled immediately."[7]

The use of scarcity has been a mainstay of attacks using digital channels, as depicted in the following email.[8]

For more information on detecting spoofed emails claiming origin from Royal Bank of Scotland, **click here.**


RBS Make it happen
The Royal Bank of Scotland
Digital Banking

Dear Valued Customer,
Due to the recent amount of fraudlent messages that targeted our customers recently. Royal bank of scotland has decided to upgrade the security of our online banking digital system. To do this we need the proper verification of each and everyone of our customers. We were unable to reach you by phone thereby sending this email as an alternative to please verify your account information by clicking on the Login button below

LOG IN

Failure to do this within 24hrs will lead to restricted access to your account for security reasons

Sorry fo the inconvience

Regards
Royal Bank Of Scotland

A phishing email employing the scarcity lever.
Source: http://www.rbs.co.uk/microsites/global/phishing_demo/.

- **Consistency:** Once targets have promised to do something, they will usually stick to their promises because they do not wish to appear untrustworthy.

  Example: "The attacker contacts a relatively new employee and advises her of the agreement to abide by certain security policies and procedures as a condition of being allowed to use company information systems. After discussing a few security practices, the caller asks the user for her password 'to verify compliance' with policy on choosing a difficult-to-guess password. Once the user reveals her password, the caller makes a recommendation to construct future passwords in such a way that the attacker will be able to guess it. The victim complies because of her prior agreement to abide by company policies and her assumption that the caller is merely verifying her compliance."[5]

- **Liking:** Targets are more likely to comply when the social engineer is someone they like.

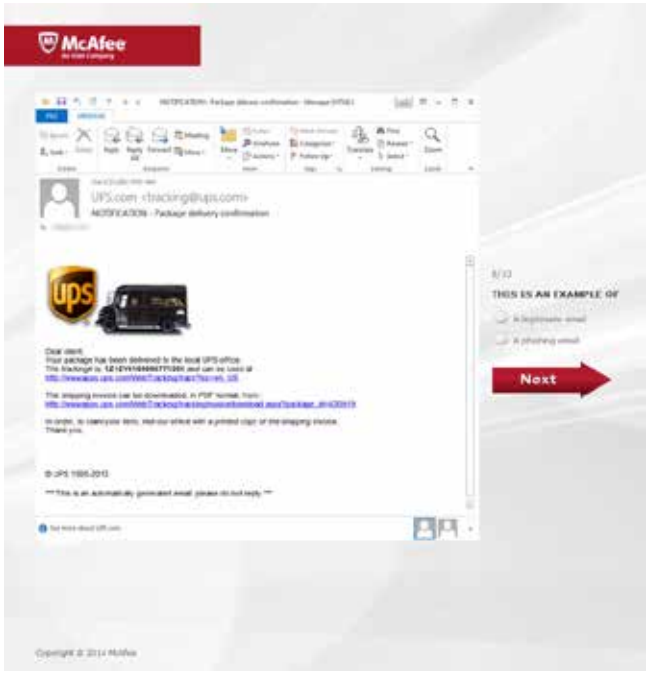
  Example: Bernard Madoff, the Wall Street trader convicted of running the biggest pyramid scheme in history (about $50 billion), reportedly used his ability to be liked as an influencing lever. "[People like Madoff] seem trustworthy because of their charm, their command of finance, and the unshakable confidence that they portray," said Jacob Frenkel, a former Securities and Exchange Commission enforcement lawyer. "The Bernie Madoffs of the world are the people you want to sit next to on an airplane."[9]

- **Authority:** People tend to comply when a request comes from a figure of authority.

  Example: The Fake President fraud was detailed by AIG in an alert: "Fraudsters impersonate a group executive (the president, CEO, or CFO, for example) and call a manager, an accounts payable clerk, or any other employee they think could be of use to their scheme in a subsidiary requesting them to execute an urgent and confidential (and generally off-shore) payment. This may well be followed up with an email (with what might appear initially to be a perfect replica of the genuine email address or an explanation of why a 'special' email address is being used)."[10]

For more information on detecting spoofed emails claiming origin from UPS, **click here.**

For typical phishing attacks, the use of authority is a common technique. Email appearing to come from a bank is common. Similarly, popular brands are imitated to deceive email recipients into taking action. In the recent **McAfee Phishing Quiz,** we found that the most successful phishing email sample appeared to be sent from UPS. The methods of disguise were common but effective. First, the sender address was spoofed to appear as if it originated from the UPS.com domain. Several UPS branding elements were part of the message, including the official logo. However, what we found most interesting was the use of only one malicious URL in the entire email. The first URL directed the recipient to track the shipment—and actually sent victims to the UPS package-tracking website. The second URL prompted a download of the "invoice," and it indeed opened a file—but not one in the UPS domain. That link delivered the payload: malware wrapped in a .zip archive.



UPS phishing email sample from the McAfee Phishing Quiz, presented in an Outlook email client.

- **Social Validation:** People tend to comply when others are doing the same thing.

  Example: "I noticed that this email had not only been sent to me but apparently to everyone in her address book, many names being familiar to me. A phone call to her confirmed my suspicion that she did not actually send the email herself, but rather some cyber-ne'er-do-well had hijacked her address book. Of course, her first question was, 'How could this happen, and what can I do?'"[11]

In this example, the sense that others are also sent the email may give the reader the feeling that it will be okay to open the email, and any links, too. This leverages social validation, as well as an element of authority because the email address itself gives the illusion it was sent from a friend.

Phase 3: Play

The play aims to carry out the purpose of the attack. It might be to extract information from the target and keep things going long enough to do so, or it might be to get the target to click on a link. Ultimately, the attacker may have a number of plays in mind. We can demonstrate a play being dragged out with the "Nigerian 419 scam." The Australian government site Scamwatch explains:

> *"Scammers ask you to pay money or give them your bank account details to help them transfer the money. You are then asked to pay fees, charges, or taxes to help release or transfer the money out of the country through your bank. These 'fees' may even start out as quite small amounts. If paid, the scammers make up new fees that require payment before you can receive your 'reward.' They will keep making up these excuses until they think they have got all the money they can out of you. You will never be sent the money that was promised."*[12]

With hunting, the play (which may be extracting information or encouraging the target to click a link) generally happens in the same interaction as the hook and exit. Although it will be a single interaction, the phases will be distinct.

Extracting information through farming happens over a longer duration. This may be over many years, and interaction with the target may be sporadic or regular. Sporadic interaction makes the pattern harder to spot because the data exfiltration patterns will be much fainter. Farming is more likely to be defeated through education, as people can learn that something they have been doing is risky.

Phase 4: Exit

The exit phase aims to close the interaction with the target. In many cases, the social engineer wishes to complete this phase without arousing suspicion. Phishing attacks typically exit without arousing suspicion. Once victims have been directed to a malicious website they believe to be genuine, they are prompted to provide the targeted information (such as login credentials). For the attack to be successful, the social engineer will provide assurances so that the victims do not become suspicious and change their passwords. For example, victims may be redirected to the original site, or be provided with a generic message to infer a technical error.

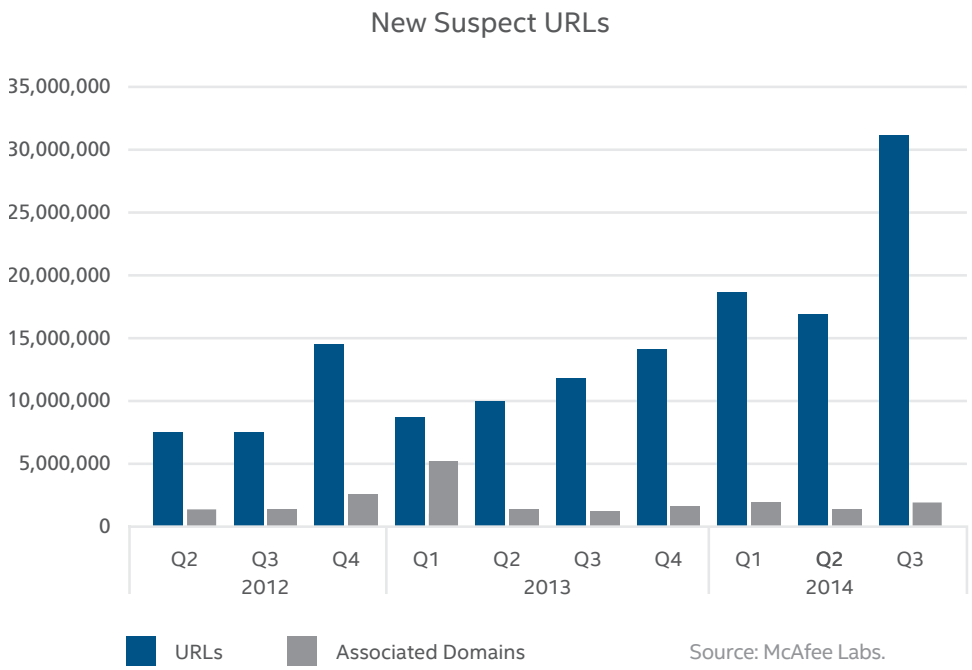
In some circumstances, the social engineer is unconcerned about arousing suspicion. This could be due to several reasons:

- **Lack of traceability:** The common practice among social engineers who hunt via telephone is to use pay-as-you-go mobiles. Upon completion of an attack (or a defined period), the mobile telephone is simply discarded.
- **Beyond the reach of law enforcement:** The social engineer conducts business from overseas locations, making it both difficult to trace and beyond the reach of law enforcement.
- **Information received:** There is no threat of the information being retracted. Some primary information is time sensitive (passwords can be reset if disclosed), but if the primary information is intellectual property, then the target cannot retract it once it is disclosed.

Social Engineering Channels of Attack

Social engineers can use several avenues for their attacks:

- **Websites:** Social engineering attacks often leverage malicious websites as a channel of attack. According to the ***2014 Verizon Data Breach Investigations Report (DBIR),*** "20% of espionage-motivated attacks use a strategic web compromise to deliver malware."[13] According to the recent ***McAfee Labs Threats Report: November 2014,*** there are millions of suspicious URLs, many of which are probably used in social engineering attacks.



The number of new suspect URLs skyrocketed in Q3 of 2014. Some of that growth can be attributed to a doubling in the number of new short URLs, which often hide malicious websites, and a sharp increase in phishing URLs.

Phishing is an attempt to acquire sensitive information through emails or instant messages that appear to be coming from a trustworthy source. The messages typically contain malware-laden attachments or links to websites that are infected with malware.

Spear phishing is an attempt directed at a specific individual or organization. Typically, a spear phishing message contains personalized information that might lead the recipient to believe that it has come from a legitimate source.

For more information on detecting spoofed emails claiming origin from PayPal, **click here.**

- **Email:** The most common forms of social engineering through email are phishing and the more targeted spear phishing. Phishing tries to acquire sensitive data from the target through social engineering (using levers such as authority, scarcity, etc.). The use of email as the communication channel is an effective method for cybercriminals because "18% of users will visit a link in a phishing email," according to the Verizon report. The three most prevalent delivery vectors for weaponized payloads by actors of advanced persistent threats, as observed by the **Lockheed Martin Computer Incident Response Team (LM-CIRT) for the years 2004–2010**, are email attachments, websites, and USB removable media.
- **Telephone:** This is a popular channel for information brokers. Text messaging is also used as a channel for attacks.

  The FBI warns the public about text-based scams designed to trick users into giving out personal information. "Be leery of emails or text messages that indicate a problem or question regarding your financial accounts. In this scam, fraudsters direct victims to follow a link or call a number to update an account or correct a purported problem."[14]
- **Face to face:** An employee can be approached and tricked or coerced into providing information.
- **Postal service:** Although this channel appears less prevalent than others, there are still reports of social engineering attacks via postal mail. Examples include the lottery scam, in which targets are asked to enter personal data onto a form and return it to claim their prize.
- **Fax:** Examples include emails posing as messages from online payment firm PayPal. They urge users to fax account information instead of the common tactic of entering details on a bogus website.

Who Are the Social Engineers?

Providing a definitive list of the malicious actors involved in social engineering for nefarious purposes is problematic. Targeted individuals or organizations will face different actors, each with their own motivations. Plus, the service-based nature of cybercrime means that a malicious actor's list of targets will depend on their clients. (For more on this topic, see the McAfee Labs report ***Cybercrime Exposed: Cybercrime-as-a-Service.)***

The types of malicious actors involved in cybercrime, any of whom may leverage social engineering as an attack vector, vary. The Center for Internet Security[15] cites the following:

- **Script kiddies:** Unskilled hackers who use simple techniques.
- **Insiders:** Although they may not have strong technical skills, their access to sensitive networks represents a risk.
- **Hacktivists:** Agents of hacktivism, which combines politics, the Internet, and other elements. Activism, a political movement emphasizing direct action, is the inspiration for hacktivism. Adding the online activity of hacking to political activism gives us hacktivism.[16]
- **Lone hackers:** Their skills or motivations will vary.
- **Organized cybercriminals:** Criminal syndicates formed to conduct cybercrime.
- **Nation-state hackers:** These actors pose the highest, consistent cyberthreat to state and territorial governments, and an unknown level of risk to local and tribal governments.
- **Terrorist groups:** The Center for Internet Security writes that skilled hackers within these groups are rare but will likely become more significant within the next one to three years as they gain a broader skill set.[17]

Other sources reference additional types of malicious actors found among legitimate organizations.

- **Private investigators:** Use pretexting, which is a social engineering technique designed to trick people into giving up personal and financial information. Criminals use the same technique to steal people's identities, according to Blogger News Network.[18]
- **Media:** "Journalists have a voracious demand for personal information, especially at the popular end of the market. The more information they reveal about celebrities or anyone remotely in the public eye, the more newspapers they can sell."[19]
- **Outsiders:** Individuals outside of an organization who work alone (not within an organized group). For example, this may include a disgruntled customer, someone related to an employee, etc. The motivation to seek data may be due to family disputes: "Privacy intrusions in matrimonial or family disputes represent another significant cause of complaints reaching the ICO, often with severe consequences for the individuals concerned."[19]

- **Commercial organizations:**
  - Insurance companies: A sector with a business incentive to acquire confidential personal data, especially information related to suspicious insurance claims.[20]
  - Lenders and creditors: "Tracing debtors is another activity which relies on good, up-to-date personal information. To recover a debt from borrowers who have defaulted on their loans or financial commitments, creditors need a current address."[19]
  - Debt collectors: "Some debt recovery firms might advertise that they use social engineering strategies to find missing overdue account holders. What that means is that the collector will use all the online information available to then go talk to neighbors, family members, business associates, and other persons to locate the missing person."[21]

Defending Against Social Engineering

Many organizations develop a user awareness program, but the effectiveness of such programs varies. One example of an ineffective training campaign comes from the United States Military Academy at West Point.

> *"Cadets at West Point receive security awareness training. The freshmen spend four hours (four lessons) learning about information assurance and network security. ... There is a culture at West Point that any email with a "COL" (abbreviation for colonel) salutation has an action to be executed. ... The email message informed cadets of a problem with their current grade report and instructed them to click on the embedded hyperlink to make sure their grade report information was correct. ... Even with four hours of computer security instruction, 90 percent of the freshmen clicked on the embedded link."*[22]

An awareness program that is combined with measures to evaluate its effectiveness is one of the best tools for fighting social engineering attacks. "The effectiveness of these controls will vary based on the quality of their implementation, including follow-up and retraining."[23]

Although continuous measurement and refinement in education programs represent an effective counter against social engineering, they are rarely used. In fact, many organizations have not implemented any sort of security or policy awareness training for their employees. A recent study by the Enterprise Management Associates (EMA) found that 56% of employees had not gone through such training.[24]

The following controls can be used to mitigate the risk of social engineering. These are divided into three categories: people, process, and technology. These controls are not exhaustive, and may not be applicable to all organizations.

People	Process	Technology
▪ **Provide clear boundaries:** All staff should be keenly aware of the policies regarding the release of information and have clear escalation paths should a request fall outside of their boundaries. ▪ **Ongoing education:** Implement a security awareness program to consistently educate employees over time. Use tools such as the McAfee Phishing Quiz to highlight specific tactics commonly used in attacks. ▪ **Permission to verify:** Provide staff with the confidence to challenge even seemingly innocuous requests. An example of this is to challenge people when attempting to tailgate into offices. ▪ **Teach the importance of information:** Even seemingly innocuous information such as telephone numbers (enabling information) can be used to stage an attack. ▪ **Create a no-blame culture:** The targets of social engineers are victims. Punishing specific employees who have been deceived will make all staff less likely to admit to releasing information. Once conned, they could come under the control of the social engineer, who can then use blackmail.	▪ **Bogus call reports:** When a suspicious activity has occurred, staff should complete a report that details the interaction. This assists investigations. ▪ **Informative block pages:** When employees reach a malicious web page, use a block page to inform them why they cannot proceed. This will cause them to reflect on their prior action and can help identify sources of attack. ▪ **Customer notification:** When callers are denied information, the organization should notify them and verify whether the caller was entitled to the information. Organizations should also consider how they communicate with customers. For example, PayPal includes guidance for users that helps identify if emails they receive are genuine: "A real email from us will never ask for your bank account number, debit, or credit card number etc. Also we'll never ask for your full name, your account password, or the answers to your PayPal security questions in an email."[25] ▪ **Escalation route:** A clear reporting line for front-line staff to escalate any doubts they may have about interacting with potentially fraudulent messages. ▪ **Tiger testing:** Routinely test staff for their susceptibility to social engineering attacks over the use of multiple communication channels. This provides a tool to measure the effectiveness of training programs.	▪ **Call recording:** Routinely record incoming telephone calls (while following federal and state wiretapping laws) to assist investigations. ▪ **Bogus lines:** Route calls that are believed to be suspicious to a monitored number. ▪ **Email filtering:** Remove fraudulent emails containing known and never-before seen malware. ▪ **Web filtering:** Block access to malicious websites and detect malware inline with access to the Internet. ▪ **Strong authentication:** Although leveraging multifactor authentication will not eliminate the risk of users being socially engineered into giving up their authentication credentials, it will make the task more difficult for would-be attackers.

Follow McAfee Labs

Summary

The threat of social engineering is very real. Cybercriminals use it to unlawfully extract information for various malicious uses. To best counter the problem, we must understand the nature of social engineering attacks. This means defining the likely threat actors, their attack methods, and their resources.

Social engineering is regarded as a low-tech attack due to the limited technical resources required to conduct an attack. Technology can be used as a control, but it cannot defeat the threat in isolation. Organizations must channel resources into education and cultural change.

About McAfee Labs

McAfee Labs is one of the world's leading sources for threat research, threat intelligence, and cybersecurity thought leadership. With data from millions of sensors across key threats vectors—file, web, message, and network—McAfee Labs delivers real-time threat intelligence, critical analysis, and expert thinking to improve protection and reduce risks. McAfee is now part of Intel Security.

www.mcafee.com/us/mcafee-labs.aspx

About Europol's European Cybercrime Centre (EC^3)

Within the framework of European Union (EU) law enforcement cooperation, Europol supports the EU member states in preventing and combating all forms of serious international crime and terrorism by means of information exchange, operational and strategic analysis, expertise, and operational support.

Europol's European Cybercrime Centre (EC^3) commenced its activities in January 2013 to strengthen the law enforcement response to cybercrime in the EU and to help protect European citizens, businesses, and governments. Its positioning within Europol means the Centre can draw on Europol's existing infrastructure and law enforcement network.

In particular, EC^3 is tasked with focusing on the following three areas:

- Cybercrimes committed by organised groups, particularly those generating large criminal profits such as online fraud.
- Cybercrimes which cause serious harm to the victim such as online child sexual exploitation.
- Cybercrimes (including cyberattacks) affecting critical infrastructure and information systems in the European Union.

About Intel Security

McAfee is now part of Intel Security. With its Security Connected strategy, innovative approach to hardware-enhanced security, and unique Global Threat Intelligence, Intel Security is intensely focused on developing proactive, proven security solutions and services that protect systems, networks, and mobile devices for business and personal use around the world. Intel Security combines the experience and expertise of McAfee with the innovation and proven performance of Intel to make security an essential ingredient in every architecture and on every computing platform. Intel Security's mission is to give everyone the confidence to live and work safely and securely in the digital world.

www.intelsecurity.com

1 **http://www.bbc.co.uk/news/technology-28106478**

2 **http://www.fedex.com/us/security/prevent-fraud/email.html**

3 **http://www.pcworld.com/article/158005/article.html**

4 **http://blogs.intel.com/energy/re-assessing-risk-energy-sector/**

5 **http://en.wikipedia.org/wiki/Robert_Cialdini**

6 Mitnick, Kevin D. & Simon, William L . "The Art of Deception" Hungry Mind Inc., 2002

7 State of Utah Department of Commerce "Media Alert" 1 December 2008
www.commerce.utah.gov/releases/08-12-11_dcp-bogus_phishing.pdf

8 **http://mindfulsecurity.com/2009/07/21/catching-a-phish/**

9 "Ponzi schemes: a primer" 23 December 2008 **http://www.tucsoncitizen.com/daily/local/105912.php**

10 **http://www.aig.com/chartis/internet/uk/eni/AIG-Fraud-alert-A4-3page-v5_tcm2538-516102.pdf**

11 **http://www.techrepublic.com/blog/user-support/hijacked-address-book-how-did-it-happen-and-what-to-do/**

12 **http://www.scamwatch.gov.au/content/index.phtml/tag/nigerian419scams**

13 **http://www.verizonenterprise.com/DBIR/2014/**

14 **http://www.fbi.gov/scams-safety/e-scams**

15 **http://msisac.cisecurity.org/resources/toolkit/oct13/documents/cyber_crime.pdf**

16 **http://www.mcafee.com/uk/resources/white-papers/wp-hacktivism.pdf**

17 **http://msisac.cisecurity.org/resources/toolkit/oct13/documents/cyber_crime.pdf**

18 **http://www.bloggernews.net/112243**

19 **http://news.bbc.co.uk/2/shared/bsp/hi/pdfs/21_07_11_icomotorman.pdf**

20 **http://venturebeat.com/2013/06/18/why-your-insurance-company-wants-to-be-friends-on-social-media/**

21 **http://www.christianet.com/debtconsolidation/commercialdebtcollector.htm**

22 **http://net.educause.edu/ir/library/pdf/eqm0517.pdf**

23 **http://www.journalofaccountancy.com/Issues/2007/Nov/TheHumanElementTheWeakestLinkInInformationSecurity.htm**

24 **http://www.scmagazine.com/study-reveals-only-56-percent-of-employees-get-awareness-training/article/342029/**

25 **https://www.paypal.com/gb/webapps/helpcenter/helphub/article/?solutionId=FAQ2061&m=HTQ**

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com