National Cybersecurity and Communications Integration Center

16 December 2015

Deception: The Art of Social Engineering

Summary

Social engineering, an age old threat, continues to play a significant role in successful attacks against people, enterprises, and agencies. The advent of the Internet, its diverse and increased use, and the reliance on it by almost every element of society, amplifies social engineering opportunities. Cybercriminals enjoy an expansive attack surface, novel attack vectors, and an increasing number of vulnerable points of entry[1]. Threat actors, both cyber and physical, continue to leverage social engineering due in part to its high rate of success. Security experts believe complex social engineering threats will continue across all vectors and attack levels will continue to intensify[2].

An observed trend in social engineering attacks is the complex and compelling nature of the engineered lure specifically targeted and sculpted for the victims using gleaned sensitive information[3,4,5,6]. Recent successful exploits resulting in large data breaches of sensitive information have contributed to a premium of available, exploitable information. Sensitive information is also readily available on corporate websites, and social media platforms such as Facebook, Twitter, LinkedIn, and others. This availability of information dramatically increases the occurrence, sophistication, and success of follow-on social engineering attacks. Clever and convincing lures tailored to the targeted individual or organization can be created by even the most unsophisticated criminal actor.

Another observed change in social engineering tactics is its inclusion in crime-as-a-service. An example of this is the tool created by China's underground cyber-crime economy[7], called "*Social Engineering Master*[8]". The tool provides access to leaked or stolen information in order to create a persuasive social engineering attack against a specific victim or group of victims. According to Eweek, Chinese cybercriminals developed this tool and it is being sold for approximately $50 on the underground market. Christopher Budd, a manager with Trend Micro, suggests that Chinese cybercriminals are becoming more sophisticated by offering services such as "*Social Engineering Master*[9]".

McAfee released a 2015 study, "*Hacking the Human Operating System, The Role of Social Engineering within Cybersecurity*[10]" which discusses the role of social engineering within cybersecurity, the lifecycle of a social engineering attack, and the psychological lures which realize the most success for attackers. This paper will discuss the McAfee and other security reports on social engineering, examples of successful social engineering attacks, and countermeasures to defend against it.

Background

Social Engineering[11]: Social engineering uses either targeted or opportunistic attacks. Typically, targeted attacks focus on a specific target while opportunistic attacks attempt to garner information from someone in a specific position such as a helpdesk technician.

> *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*[12].

McAfee divided social engineering into two categories: farming and hunting.

> Cybercriminals use "*hunting"* when attempting to glean information with minimal interaction between themselves and their victims. Malicious emails containing targeted or general lures such as Spoofed FedEx or shipping-themed emails are examples of *hunting.*
>
> "*Farming"* is defined as the technique used by cybercriminals to create a relationship with the targeted entity and then attempt to glean information from the entity over a longer duration of time. Creating faked LinkedIn and Facebook profiles are cybercriminal *farming* tactics used to establish trusted relationships in order to glean information from targets. *Farming*, while not as prevalent as *hunting*, has increased.

The duration of social engineering attacks varies and may consist of a single telephone call, email, or direct message (hunting) or it may span many years (farming) with ongoing interactions. Its focus is to gather useable information in order to exploit individuals or as a broader campaign in an attempt to compromise a larger target. Currently, cybercriminals do not require extensive technical abilities or capabilities to successfully target and exploit human vulnerabilities[13].

Social Engineering Phases: Criminals gain access to victims' accounts using a variety of customizable social engineering methods. McAfee outlines this process into four phases[14]:

1. ***Research*** is used to garner information that may assist in identifying and compelling the target to observe an unsafe practice. The Internet allows cybercriminals to remotely conduct open source research using websites, social network profiles, public documents, and other available resources. Some of the information sought includes phone numbers, Internet Service Providers (ISPs), addresses, and other publicly available information. In addition to online research, attackers may socialize or physically interact with the target. In opportunistic attacks, the actor may conduct little to no research.
2. ***Hook*** is when cybercriminals attempt to compromise targeted individuals or groups. Robert Cialdini discusses in "*The Psychology of Persuasion*" six possible "levers" that can be used to hook the targeted individual or group[15]. The influencing levers are reciprocation, commitment and consistency, social

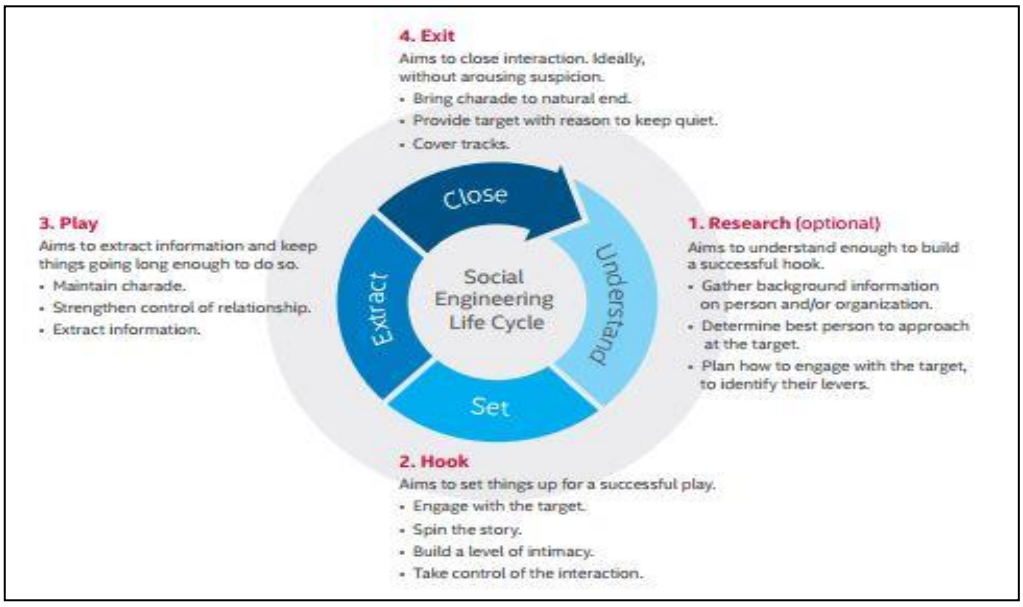

Figure 1: 4 Phases of a Social Engineering Attack, provided by McAfee

validation, like-ability, authority, and scarcity. This is the phase where the attacker involves the target, creates the spoof, builds trust, and compromises the target.

3. ***Play*** is the extraction of information and maintaining control of the situation. This phase is where the user clicks on the malicious link, provides personal or financial information, or pays money. Sometimes the hook and play phases occur simultaneously.
4. ***Exit*** is closing the link with the targeted victim and completing the scam without arousing suspicion.

Social Engineering Attack Vectors[16]:

Email: Is the most common attack vector of social engineering. There are different types of social engineering emails to include phishing, spear-phishing (targeted phishing), and whaling (emails targeting high-profile individuals or certain groups of interest to the criminals). The sensitive information obtained by malicious emails often uses the authority or scarcity levers described in the McAfee report. A threat report from Quick Heal identified that in the third quarter of 2015, the number of spam emails categorized as malicious, spiked with approximately 36 percent of all emails including a tracking cookie, malicious attachment or URL, or malware designed to infect the receiver's computer[17].

Websites[18]: Social engineering attacks leverage malicious or compromised websites. The extent and severity of malicious URLs used for social engineering is highlighted in the McAfee report. Also striking is the OWASP website report on the "*Top 10 2013-A10-Unvalidated Redirects and Forwards*[19]*"*. Attackers strategically select websites identified to be of interest to their target for the purpose of compromising the website in order to infect the targeted victim with malware. Malvertising Campaigns, such as the recent "*Casino Malvertising Campaign*[20]" are also used. The Casino Malvertising campaign logged over 1 million visitors which may have spread malware to unsuspecting victims.

Malvertising is the compromise of online advertising networks.

Telephone: The telephone is often used by malicious information brokers. The Federal Bureau of Investigation (FBI) recently warned of a new phone scam where the caller impersonates a Department of Energy (DoE) or FBI employee to inform them of a case against them. The FBI states it is not standard practice to call individuals to inform them of a case against them[21]. In this scam, fraudsters direct victims to follow a link or call a number to update an account or correct a purported problem.[22]"

Text Messaging: Used by malicious information agents as another channel to gather information to compromise their target. The FBI warns of scams designed to trick users into giving out personal information and to be leery of emails or text messages that indicate a problem or question regarding your financial accounts[23].

Social Media Engineering: Social media provides a one-to-many attack surface, which has the capability to significantly enlarge attack avenues. The collection and sharing of data and the ability to use that data for further compromise is greatly enhanced through the variety of social media platforms[24]. Some examples include fake LinkedIn profiles[25,26] or the information available both legitimately[27] or compromised[28] on Facebook accounts.

Face-to-face: An employee can be approached and deceived or coerced into providing information directly.

Postal Service[29]: This vector is not used as often as other social engineering attack vectors, but some examples include Lottery or Fake Check scams.

Social Engineering Channels of Attacks[30] include an array of malicious diversions. Common methods include***:***

- ***Phishing*** - Probably the most common form of social engineering attack; is used to collect personal information from victims, such as names, addresses and social security numbers;
- ***Spearphishing*** - A form of phishing which uses tailored techniques to lure the targeted victim;
- ***Whaling*** - Spearphishing of high profile individuals or members of certain groups of interest to the criminals;
- ***Pretexting***[31]- Is when an individual lies to obtain privileged data by concocting scenarios or creating a pretense in order to steal the victim's personal data or to gain access to victim's system. These attacks typically are when the actor pretends to have or need certain pieces of information. A high level example of pretexting includes the multi-step scam in which an actor stole the Twitter handle from Naoki Hiroshima's @N[32]. The attacker called the helpdesk of GoDaddy; using information collected prior to the call to convince the helpdesk employee to redirect Naoki's email to the attacker. The attacker did not have all the information needed to identify himself as Naoki, but managed to dupe the employee into giving up the account password;
- ***Baiting*** - A form of social engineering used by hackers that entice victims with the promise of an item or good. Baiters may offer users free music or movie downloads, if they surrender their login credentials to a certain website. Baiting attacks are not confined to online schemes. Attackers can also focus on exploiting human curiosity through use of physical media such as an attack using strategically placed, infected USBs;
- ***Quid Pro Quo*** - A form of social engineering that promises a benefit in exchange for information. These benefits are typically in the form of a service. The most common use of this technique involves miscreants who pose as information technology (IT) service personnel and spam call as many individuals and companies as possible with promises to provide free IT support in exchange for the victim's commitment to purchase anti-virus software;
- ***Tailgating or "Piggybacking"*** - A form of social engineering involving someone who lacks the proper authentication and authorization who follows another person into a restricted area. An example of a tailgating attack is when a person impersonates a delivery driver and waits outside a building. When an employee gains security's approval and opens the door, the attacker asks that the employee hold the door, thereby gaining unauthorized access to the building.

Malicious Social Engineers[33] come in all shapes and sizes, making it difficult to create a conclusive list and profile of these nefarious actors. The actors' motivation, skill levels, and desired targets often reflect the type of malicious social engineer. That said, the following types of actors who use social engineering could include; script kiddies, insiders, hacktivists, organized cybercriminals, nation-state actors, and terrorist groups. Another, not so obvious, list includes actors within legitimate organizations such as private investigators and media personnel.

Examples of Observed Social Engineering Attacks

Social engineering[34] uses human interaction (social skills) to obtain or compromise information about user(s), organization(s), or associated computer systems. An attacker may seem unassuming and respectable; possibly claiming to be a new employee, repair person, or researcher; or possibly offering credentials to support his or her identity. The cyber social engineer asks questions, pieces together enough

information to compel a victim into acting upon an unsafe or unusual practice that facilitates the infection process or compromise. As explained in numerous WASPs[35] it is often unfair to blame the victim with some studies indicating that more than 80 percent of people studied were unable to detect the most common and frequently used phishing scams[36]. Some observed social engineering attacks follow:

Telecommunications Service Providers[37]: Recent reports reveal a trend in criminal actors conducting social engineering scams that target phone and email service providers. Perpetrators have called U. S. telecommunication companies' technical support number and posed as an internal technical support representative from another call center. The perpetrator then explains that the system is down at their particular location and asks the company employee to retrieve customer information in their system based on partial information provided by the perpetrator. The miscreant then manipulates the employee into disclosing information that allows access to the business customer's online account. The information can be used to commit identity theft and facilitate various fraud schemes.

High Ranking Government Officials[38,39]: In an interview with Wired, the teen, who claims to have compromised CIA Director Brennan's personal AOL email account, explained the compromise. The first step of the compromise consisted of the actor doing a reverse lookup of Director Brennan's mobile phone number, enabling him to determine the ISP [40] that Director Brennan used. Once that was determined, the actor impersonated a technician from the ISP in order to obtain details of Director Brennan's account. The actor claims to have gleaned Director Brennan's account number, his four-digit PIN, the backup mobile number on the account, Director Brennan's AOL email address, and the last four digits on his bank card. The actor then asserts he impersonated Director Brennan and called the AOL helpdesk claiming to be locked out of his account. Leveraging prior information, the actor was able to answer or cleverly discuss the security questions for the account with the helpdesk. The helpdesk was tricked into resetting the password to the AOL email account giving the actor access. The compromise, according to Wired, occurred on 12 October 2015, and lasted for three days before the account was shutdown.

In a similar incident, the same actor claimed to have used similar techniques to compromise DHS Secretary Jeh Johnson's personal email and White House Deputy National Security Advisor Avril Haines' personal email[41].

Fake LinkedIn Profiles[42]: Social networking platforms are increasingly being used by malicious actors to glean information, according to Symantec[43]. Access to LinkedIn accounts offers malicious actors with diverse motivations the ability to engage and identify targets. A Trusted Third Party has identified espionage groups carrying out reconnaissance and intrusion activities. An example of this could be the Iran-based Newscaster team which targeted public and private sectors in the United States (U.S.), the U.K., Israel, and others using social media[44,45].

Healthcare[46]: One sector that has identified a recent growth in identity theft is healthcare[47]. This growth is due in part to the increased opportunities to commit medical identity theft and fraud as patient records are digitized. Cybercriminals appear to be quite effective at aggregating patient identity data through the use of stolen medical records and other data mining avenues such as social engineering. These fraudulent medical identities can then be readily exploited and misused for dispensing fraudulent medical treatment and care by an impostor, thus making the victim's medical record inaccurate and augurs the potential for medical risk.

Comptroller Email Scam[48]: According to CSOonline, an International Data Group company experienced a near-perfect social engineering attack that was spoiled by a single mistake. An email was allegedly sent to the company's comptroller from the CEO requesting the comptroller

release payments expeditiously. The email mirrored the organization's Outlook template and had a similar tone of other emails from the CEO. The one difference noticed by the comptroller was that the email was signed with the full name of the CEO who never used his full name. In this case; awareness, training, and an atmosphere of acceptance to question suspicious requests allowed the comptroller to discover the scam.

Social Engineering Countermeasures

As explained in a previous WASP article[49] and other security resources it is beneficial to create a culture of cybersecurity rather than blame the victims[50] of social engineering. A trend of explicitly tailored social engineering attacks makes it difficult for even the most sophisticated user to identify malicious lures. The increased use of the Internet and changes to technology broaden attack surfaces, and provide new attack vectors, further increasing the difficulty for users to identify scams. The continued use of social engineering attacks indicate that user awareness and user training are not a panacea in preventing successful social engineering attacks[51]. However, the following countermeasures may be put in place to counter the risks of social engineering[52]. These countermeasures stretch across three categories: people, process, and technology:

People[53]:

- Even though user awareness training is not the panacea that prevents social engineering, IT security specialists should ensure users are trained properly. Companies should employ, at minimum, bi-annual training geared towards each user group (end-users, IT staff, managers, etc.) so that everyone is aware of the latest attacks. This includes conducting social engineering tabletop exercises to keep personnel vigilant to avoid attacks and employing evaluation methods such as the McAfee Phishing Quiz[54]. This training should also include measurements to evaluate effectiveness and retraining requirements;
- Clearly define and strictly enforce policies regarding the release of information and set clear escalation paths should a request for information fall outside those policies;
- Institute a "No Blame" policy for those targeted by social engineering. Punishing or shaming those who are victims decreases the likelihood that victims will notify the proper authorities in instances in which they have been conned;
- Set a climate which promotes "Permission to Verify" such as challenging people when attempting to tailgate into offices or questioning emails requesting information;
- Clearly explain the importance of information. Even the most innocuous information can be used for social engineering;
- Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company;
- Password protect your phone records by calling your phone company or provider;
- Request that companies use something other than your social security number or obvious questions/responses for the security questions set for the account;
- If there is doubt about how safe a link or website is; there are multiple on-line tools available from various security vendors such as "*TrustedSource*[55]" or "*SiteAdvisor*[56]" from McAfee, Norton's *SafeWeb*[57], *PhishTank*[58], or VirusTotal[59];
- Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information;
- Do not reveal personal or financial information in emails and do not respond to email solicitations for this information. This includes following links sent in emails;

- Do not send sensitive information over the Internet before checking a website's security (see a Protecting Your Privacy White Paper from Global Knowledge[60] for more information);
- Pay attention to the URL of a website. Malicious websites may look identical to a legitimate website, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net). Also pay attention to shortened links that can camouflage the actual location of the website;
- If you are unsure whether an email request is legitimate, attempt to verify it by contacting the company directly. Do not use contact information provided on a website connected to the request; instead, check previous statements for contact information. Information about known phishing attacks is also available online from groups such as the Anti-Phishing Working Group[61].

Process[62]:

- Institute tracking procedures such as "Bogus Call Reports" that can be used to detail fraudulent interaction;
- Provide detailed information on why a web page is blocked. If an employee tries to access a malicious web page clearly inform the employee of why the website is blocked. This information increases employee awareness;
- Clearly communicate with customers what to expect and what not to expect in email requests, phone calls, or from company websites. Include guidance as to what will be asked or not asked via these channels. If a customer is denied information, establish a follow-up procedure to verify whether or not the individual was entitled to the information;
- Establish an clear escalation route for individuals and supervisors to use when interacting with fraudulent communications;
- Implement "Tiger Testing" procedures to test the susceptibility of users to social engineering attacks.

Technology[63]**:**

- Put Spam and Virus email filters in place that block fraudulent emails containing phishing exploits and malware before they reach internal servers;
- Filter malicious websites;
- Deployment of an endpoint protection system can be used to block the latest malware;
- Deploy an Intrusion Prevention System (IPS) solution that detects known attacks and the level of network access based on signature and behavior;
- Monitor and record incoming calls to assist with investigations. Always follow federal and state wiretapping laws. Route bogus call numbers to a monitored number;
- Leverage multi-factor authentication for verification of identity.

What to do if you think you are a victim[64]:

- If you believe you might have revealed sensitive information about your organization, report it to the appropriate people within the organization, including network administrators. They can monitor for any suspicious or unusual network activity;
- If you believe your financial accounts may be compromised, contact your financial institution immediately and close any accounts that may have been compromised. Watch for any unexplainable charges to your account;
- Immediately change any passwords you might have revealed. If you used the same password for multiple resources, make sure to change it for each account, and do not use that password in the future;
- Watch for other signs of identity theft, see *Preventing and Responding to Identity Theft*[65] for more information;

- Consider reporting the attack to the police and filing a report with the Federal Trade Commission[66];
- Consider contacting the Federal Bureau of Investigation Internet Crime Complaint Center (IC3)[67].

Conclusion

Cyber attackers are motivated and clever using a multitude of tactics and techniques. Malicious social engineering is and will continue to be widespread and used as a significant means of attacking anyone and everything connected to the Internet. In order to combat social engineering techniques and tactics, organizations must channel tiered resources; implementing an educational and cultural change and maximize the use existing technology controls.

Who Can I Share This With?

As a reminder, Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels.

Contact Information:

Any questions regarding this advisory can be directed to DHS NCCIC and to be added to the normal distribution for similar products, please send requests to NCCIC@hq.dhs.gov or (888) 282-0870.

[1] EC3 Europol Input; accessed on 3 December 2015; http://www.mcafee.com/us/resources/reports/rp-hacking-human-os.pdf
[2] EC3 Europol Input; accessed on 3 December 2015; http://www.mcafee.com/us/resources/reports/rp-hacking-human-os.pdf
[3] EC3 Europol Input; accessed on 3 December 2015; http://www.mcafee.com/us/resources/reports/rp-hacking-human-os.pdf
[4] Experts gather at INTERPOL to identify emerging social engineering fraud techniques; accessed on 4 December 2015; http://www.interpol.int/News-and-media/News/2015/N2015-204
[5] Techniques, Lures, and Tactics to Counter Social Engineering Attacks; accessed on 2 December 2015; http://www.darkreading.com/partner-perspectives/intel/techniques-lures-and-tactics-to-counter-social-engineering-attacks-/a/d-id/1319401
[6] Social engineering attacks more complex than ever, says expert; accessed on 8 December 2015; http://www.computerweekly.com/news/4500247025/Social-engineering-attacks-more-complex-than-ever-says-expert
[7] Prototype Nation, The Chinese Cybercriminal Underground in 2015; accessed on 8 December 2015http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-prototype-nation.pdf
[8] China's Underground Cyber-Crime Economy Grows in Size, Sophistication; accessed on 3 December 2015; http://www.eweek.com/security/chinas-underground-cyber-crime-economy-grows-in-size-sophistication.html
[9] Prototype Nation: Innovations in the Chinese Cybercriminal Underground; accessed on 6 December 2015; http://blog.trendmicro.com/prototype-nation-innovations-in-the-chinese-cybercriminal-underground/
[10] Hacking the Human Operating System, The Role of Social Engineering within Cybersecurity; accessed on 2 December 2015; http://www.mcafee.com/us/resources/reports/rp-hacking-human-os.pdf
[11] Hacking the Human Operating System, The Role of Social Engineering within Cybersecurity; accessed on 2 December 2015; http://www.mcafee.com/us/resources/reports/rp-hacking-human-os.pdf
[12] Hacking the Human Operating System, The Role of Social Engineering within Cybersecurity; accessed on 2 December 2015; http://www.mcafee.com/us/resources/reports/rp-hacking-human-os.pdf
[13] Internet Organized Crime Threat Assessment (iOCTA) 2014; European Cyber Crime Center; accessed on 2 December 2015;
[14] Hacking the Human Operating System, The Role of Social Engineering within Cybersecurity; accessed on 2 December 2015; http://www.mcafee.com/us/resources/reports/rp-hacking-human-os.pdf
[15] Insights on Integrated Marketing Communication; accessed on 3 December 2015; http://buytheway.annenbergcourse.org/persuasion-in-advertising-6-ways-to-hook-your-customer/
[16] Hacking the Human Operating System, The Role of Social Engineering within Cybersecurity; accessed on 2 December 2015; http://www.mcafee.com/us/resources/reports/rp-hacking-human-os.pdf
[17] Quick Heal Technologies' Quarterly Threat Report Reveals Extent of Malicious Emails and Malware Plaguing Organizations Worldwide; accessed on 3 December 2015; http://bitcast-b.bitgravity.com/quickheal/documents/others/quick_heal_quarterly_threat_report_Q3_2015.pdf
[18] US-CERT Alerts Users to Holiday Phishing Scams and Malware Campaigns; accessed on 3 December 2015; https://www.us-cert.gov/ncas/current-activity/2015/11/25/US-CERT-Alerts-Users-Holiday-Phishing-Scams-and-Malware-Campaigns
[19] Top 10 2013-A10 Unvalidated Redirects and Forwards; accessed on 3 December 2015; https://www.owasp.org/index.php/Top_10_2013-A10-Unvalidated_Redirects_and_Forwards
[20] The Casino Malvertising Campaign; accessed on 3 December 2015; https://blog.malwarebytes.org/malvertising-2/2015/11/the-casino-malvertising-campaign/
[21] FBI warns of phone scam making its way to St. Joseph, Michigan area; accessed on 3 December 2015; http://www.fox28.com/story/30595894/2015/11/24/fbi-warns-of-phone-scam-making-its-way-to-st-joseph-michigan-area or http://www.bing.com/search?q=FBI+Phone+Scam&FORM=R5FD1
[22] FBI E-Scams Report; accessed on 3 December 2015; http://www.fbi.gov/scams-safety/e-scams

[23] FBI E-Scams Report; accessed on 3 December 2015; http://www.fbi.gov/scams-safety/e-scams
[24] Social Media Engineering: the Art of Hacking Humans; accessed on 3 December 2015; https://www.zerofox.com/blog/social-media-engineering-the-art-of-hacking-humans/
[25] The Anatomy Of A FAKE LinkedIn Profile; accessed on 4 December 2015; https://www.linkedin.com/pulse/anatomy-fake-linkedin-profile-andy-foote
[26] Hackers use fake LinkedIn profiles to target users; accessed on 3 December 2015; http://myinforms.com/en-us/a/20116436-hackers-use-fake-linkedin-profiles-to-target-users/
[27] Facebook Hacks Your Brain; Brief History of Social Media Science; accessed on 4 December 2015; http://www.vocativ.com/news/249354/facebook-hacks-your-brain/
[28] Facebook Notifies State Department Employees of Iran Hacks; accessed on 4 December 2015; http://www.newsweek.com/facebook-notifies-state-department-employees-iran-hacks-398296
[29] How to Contact the U.S. Postal Inspection Service; accessed on 3 December 2015; http://about.usps.com/publications/pub300a/pub300a_tech_024.htm
[30] Hacking the Human Operating System, The Role of Social Engineering within Cybersecurity; accessed on 2 December 2015; http://www.mcafee.com/us/resources/reports/rp-hacking-human-os.pdf
[31] Pretexting: How to avoid social engineering scams; accessed on 3 December 2015; http://searchsecurity.techtarget.com/answer/Pretexting-How-to-avoid-social-engineering-scams
[32] GoDaddy Admits Hacker's Social Engineering Led It To Divulge Info In @N Twitter Account Hack; accessed on 3 December 2015; http://techcrunch.com/2014/01/29/godaddy-admits-hackers-social-engineering-led-it-to-divulge-info-in-n-twitter-account-hack/
[33] Hacking the Human Operating System, The Role of Social Engineering within Cybersecurity; accessed on 2 December 2015; http://www.mcafee.com/us/resources/reports/rp-hacking-human-os.pdf
[34] Security Tip (ST04-014); accessed on 1 December 2015; https://www.us-cert.gov/ncas/tips/ST04-014
[35] 201511_WASP, 20151124_WASP
[36] Intel Security warns of six social engineering techniques targeting businesses; accessed on 3 December 2015; http://www.computerweekly.com/news/2240240671/Intel-Security-warns-of-six-social-engineering-techniques-targeting-businesses
[37] Trusted Third Party
[38] Teen Who Hacked CIA Director's Email Tells How He Did It; accessed on 2 December 2015; http://www.wired.com/2015/10/hacker-who-broke-into-cia-director-john-brennan-email-tells-how-he-did-it/
[39] NCCIC Product, Hacker(s) Claimed Control of Senior Executives' Email Accounts; accessed on 3 December 2015;
[40] Teen Who Hacked CIA Director's Email Tells How He Did It; accessed on 2 December 2015; http://www.wired.com/2015/10/hacker-who-broke-into-cia-director-john-brennan-email-tells-how-he-did-it/
[41] Teen Who Hacked CIA Director's Email Tells How He Did It; accessed on 2 December 2015; http://www.wired.com/2015/10/hacker-who-broke-into-cia-director-john-brennan-email-tells-how-he-did-it/
[42] 20151015_WASP;Iran Based Hacker Group Faked LinkedIn Profiles; accessed on 4 December 2015
[43] Fake LinkedIn profiles used by hackers; accessed on 4 December 2015; http://www.bbc.com/news/technology-34994858
[44] 20151015_WASP
[45] Newscaster – An Iranian Threat Inside Social Media; accessed on 3 December 2015; http://www.isightpartners.com/2014/05/newscaster-iranian-threat-inside-social-media/
[46] 20150311_WASP
[47] Why Medical ID Fraud is Rapidly Growing, accessed on 26 February 2015; http://www.healthcareinfosecurity.com/interviews/medical-id-fraud-rapidly-growing-i-2593?rf=2015-02-26-eh&utmsource=SilverpopMailing&utmmedium=email&utmcampaign=enews-his-20150226%20(1)&utmcontent=&spMailingID=7537918&spUserID=NzAyMDA5NDk3NzcS1&spJobID=622488769&spReportId=NjIyNDg4NzY5S0
[48] Near-flawless Social Engineering attack spoiled by single flaw; accessed on 3 December 2015; http://www.csoonline.com/article/2990471/social-engineering/near-flawless-social-engineering-attack-spoiled-by-single-flaw.html
[49] 20151111_WASP
[50] Intel Security warns of six social engineering techniques targeting businesses; accessed on 3 December 2015; http://www.computerweekly.com/news/2240240671/Intel-Security-warns-of-six-social-engineering-techniques-targeting-businesses
[51] 20151111_WASP
[52] Social Engineering Attacks: Common Techniques & How to Prevent an Attack: accessed on 1 December 2015; https://digitalguardian.com/blog/social-engineering-attacks-common-techniques-how-prevent-attack
[53] Hacking the Human Operating System, The Role of Social Engineering within Cybersecurity; accessed on 2 December 2015; http://www.mcafee.com/us/resources/reports/rp-hacking-human-os.pdf
[54] McAfee Phishing Quiz; accessed on 3 December 2015; https://phishingquiz.mcafee.com/home/hthos
[55] Trusted Source McAfee; accessed on 3 December 2015; https://www.trustedsource.org/
[56] McAfee Webadvisor; accessed on 3 December 2015; http://home.mcafee.com/root/landingpage.aspx?lpname=get-it-now&affid=0&cid=170789
[57] Norton Safe Web; accessed on 3 December 2015; https://safeweb.norton.com/
[58] PhishTank; accessed on 4 December 2015; http://www.phishtank.com/index.php
[59] VirusTotal; accessed on 4 December 2015; https://www.virustotal.com/
[60] Technology Offers Convenience, Privacy Pays the Price; accessed on 11 December 2015; http://images.globalknowledge.com/wwwimages/whitepaperpdf/WP_DataPrivacy.pdf
[61] Ant phishing Checkpoint; accessed on 3 December 2015; http://www.antiphishing.org)
[62] Hacking the Human Operating System, The Role of Social Engineering within Cybersecurity; accessed on 2 December 2015; http://www.mcafee.com/us/resources/reports/rp-hacking-human-os.pdf
[63] Hacking the Human Operating System, The Role of Social Engineering within Cybersecurity; accessed on 2 December 2015; http://www.mcafee.com/us/resources/reports/rp-hacking-human-os.pdf
[64] Avoiding Social Engineering and Phishing Attacks; accessed on 3 December 2015; https://www.us-cert.gov/ncas/tips/ST04-014
[65] Avoiding Social Engineering and Phishing Attacks; accessed on 3 December 2015; https://www.us-cert.gov/ncas/tips/ST04-014

[66] Federal Trade Commission Reporting; accessed on 3 December 2015; (http://www.ftc.gov/
[67] FBI Internet Crime Complaint Center (IC3); accessed on 3 December 2015; http://www.ic3.gov/media/default.aspx

OMB Control No.: 1670-0027
Expiration Date: 10/31/2017

UNCLASSIFIED

Homeland Security

National Protection and Programs Directorate

NPPD Customer Feedback Survey

Product Title:

1. Please select the partner type that best describes your organization. Select One

2. Overall, how satisfied are you with the usefulness of this product?

- ◯ **Very Satisfied**
- ◯ **Somewhat Satisfied**
- ◯ **Neither Satisfied Nor Dissatisfied**
- ◯ **Somewhat Dissatisfied**
- ◯ **Very Dissatisfied**

3. How did you use this product in support of your mission?

- ☐ Integrated into one of my own organization's information or analytic products
- ☐ Used contents to improve my own organization's security or resiliency efforts or plans
  - If so, which efforts?
- ☐ Shared contents with government partners
  - If so, which partners?
- ☐ Shared contents with private sector partners
  - If so, which partners?
- ☐ Other (please specify)

4. Please rank this product's relevance to your mission. ***(Please portion mark comments.)***

- ◯ Critical
- ◯ Very Important
- ◯ Somewhat Important
- ◯ Not Important
- ◯ N/A

5. Please rate your satisfaction with each of the following:

	Very Satisfied	**Somewhat Satisfied**	**Somewhat Dissatisfied**	**Very Dissatisfied**	**N/A**
Timeliness of product or support	◯	◯	◯	◯	◯
Relevance to your information needs	◯	◯	◯	◯	◯

6. How could this product or service be improved to increase its value to your mission? ***(Please portion mark comments.)***

To help us understand more about your organization so we can better tailor future products, please provide (OPTIONAL):

Name:
Organization:
Contact Number:
Position:
State: Select One
Email:

SUBMIT FORM

Privacy Act Statement

Paperwork Reduction Act Compliance Statement

UNCLASSIFIED

REV: 3 March 2015