Software Engineering Institute

Unintentional Insider Threats: A Review of Phishing and Malware Incidents by Economic Sector

Produced for
Department of Homeland Security
Federal Network Resilience Cybersecurity Assurance Branch

CERT® Insider Threat Team

July 2014

TECHNICAL NOTE
CMU/SEI-2014-TN-007

CERT® Division

http://www.sei.cmu.edu

Carnegie Mellon University

This material is based upon work funded and supported by Department of Homeland Security under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Department of Homeland Security or the United States Department of Defense.

This report was prepared for the
SEI Administrative Agent
AFLCMC/PZM
20 Schilling Circle, Bldg 1305, 3rd floor
Hanscom AFB, MA 01731-2125

DM-0001462

Table of Contents

List of Figures

List of Tables

Acknowledgments

The Department of Homeland Security (DHS) Office of Federal Network Resilience (FNR) sponsored this research and the publishing of this report.

The Insider Threat team would like to thank Tracy Cassidy and Matthew Collins, team members of the CERT Insider Threat Center, for their integral contributions to this report.

Executive Summary

The CERT® Insider Threat Center, part of Carnegie Mellon University's Software Engineering Institute, is continuing its research into the unintentional insider threat (UIT). Previous products in this line of inquiry include the foundational study for UIT[1] and the study of UIT cases involving social engineering.[2]

The current body of work looks deeper at social engineering cases involving malware or spyware. This research has produced a new category of UIT threat vector, PHISHING/SOCIAL, which replaces UIT-HACK, previously established in the UIT foundational study. The PHISHING/SOCIAL vector comprises two subvectors: Malware (formerly UIT-HACK) and Credentials. The team also examined the industries impacted by PHISHING/SOCIAL cases, the kinds of incidents involving this threat vector, and the complexity of the attacks. This report provides an initial review of particular industrial sectors by type of incident involving the PHISHING/SOCIAL threat vector. While establishing models and mitigation strategies will require further research, this report offers initial recommendations for collection and analysis of PHISHING/SOCIAL incidents in organizations.

Defining and Characterizing UIT

The following terms and definitions are related to UIT.

unintentional insider threat (UIT):

> *An unintentional insider threat is (1) a current or former employee, contractor, or business partner (2) who has or had authorized access to an organization's network, system, or data and who, (3) through action or inaction without malicious intent, (4) unwittingly causes harm or substantially increases the probability of future serious harm to the confidentiality, integrity, or availability of the organization's resources or assets, including information, information systems, or financial systems.*

PHISHING/SOCIAL, Malware:

> *An outsider's electronic entry acquired through social engineering (e.g., phishing email incident, planted or unauthorized USB drive) and carried out via software, such as malware and spyware.*

[®] CERT® is a registered mark owned by Carnegie Mellon University.

[1] CERT Insider Threat Team. *Unintentional Insider Threats: A Foundational Study* (CMU/SEI-2013-TN-022). Software Engineering Institute, Carnegie Mellon University, 2013. http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=58744

[2] CERT Insider Threat Center. *Unintentional Insider Threats: Social Engineering* (CMU/SEI-2013-TN-024). Software Engineering Institute, Carnegie Mellon University, 2014. http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=77455

PHISHING/SOCIAL, Credentials:

> *An outsider's electronic entry acquired through social engineering (e.g., phishing email incident) and carried out through compromised credentials, including passwords and other identifying information.*

The research showed that malware incidents are often linked to the PHISHING/SOCIAL threat vector.

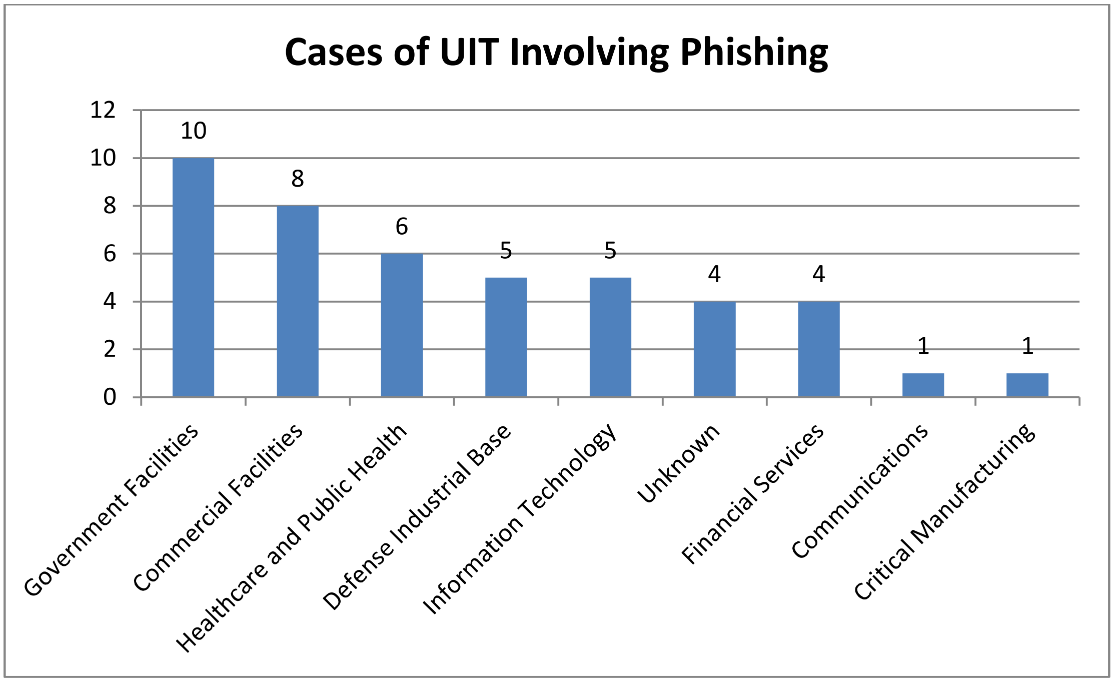
Differentiating Between PHISHING/SOCIAL and Malware (Formerly UIT-HACK)

Through the study of UIT-HACK incidents, we identified a new threat vector, PHISHING/SOCIAL, and its two subvectors, Malware and Credentials. The two subvectors share a common vector of phishing or other social engineering, which gives the attacker unauthorized access, but they differ in the weapon the attacker uses to carry out the rest of the attack: software (Malware) or the victim's credentials (Credentials).

The creation of this new category of threat vector and its two subvectors allows researchers and operations staff to quickly and precisely identify the vector of an incident so they can take the appropriate mitigation actions.

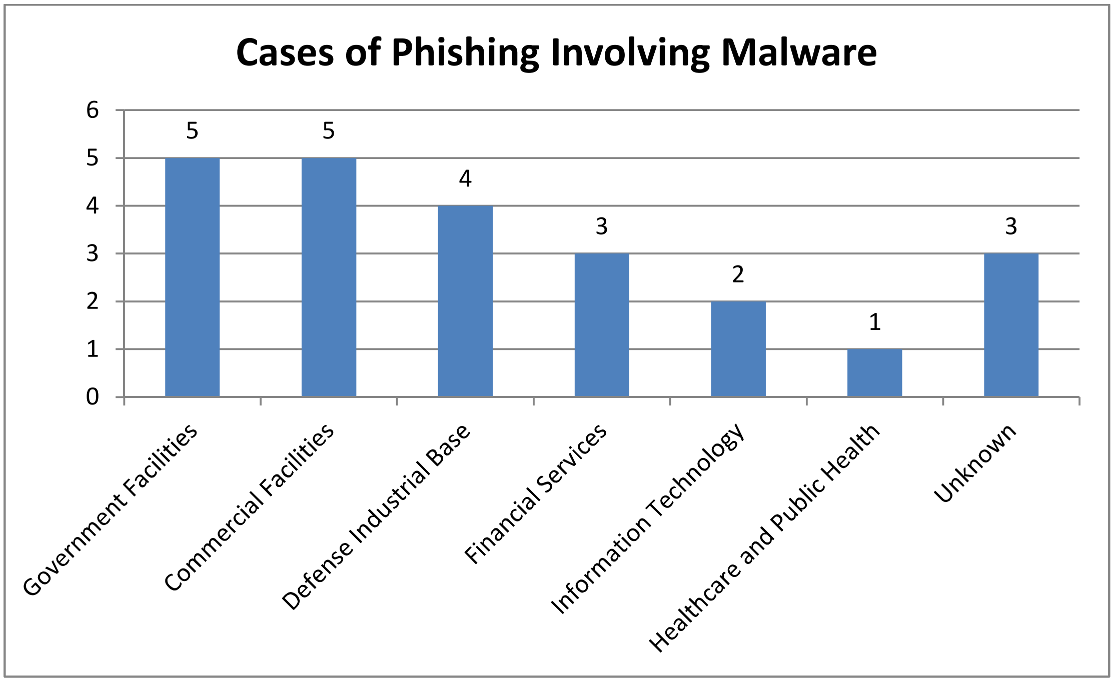
Research Findings on PHISHING/SOCIAL Threat Incidents by Economic Sector

Within the CERT Insider Threat Center's UIT corpus of 110 cases, this research identified 44 PHISHING/SOCIAL cases. These incidents are broken down by U.S. economic sector in the following chart.



Research Findings on Malware Threat Vectors and Economic Sectors

The Malware subvector of the PHISHING/SOCIAL vector offers a compelling area of research because of the high stakes this kind of incident entails. In the absence of malware, an organization could simply lose credentials, usually to a confined service, as is common with the PHISHING/SOCIAL threat vector. However, malware could compromise the entire network, putting far more than credentials at risk of alteration, deletion, or theft. Organizations experiencing a malware incident may choose to mitigate it differently than if malware was not involved. Of the 44 PHISHING/SOCIAL cases identified, 23 were malware cases. These cases are broken down by U.S. economic sector in the following chart.



Case Studies, Characteristics, and Patterns of Threat Vector by Economic Sector

Looking deeper into both the PHISHING/SOCIAL threat vector and the Malware subvector, the CERT Insider Threat Center team assessed whether these incidents constituted single-stage or multi-stage events.[3] Then the team cross-referenced the results of this research by which sector experienced which type of incidents. Due to the small sample of cases available, this report does not definitively declare if certain sectors should focus on one type of incident or the other. Instead, it draws some initial conclusions to suggest further areas of research to help make that determination in the future.

[3] For details on single- and multi-stage incidents, see Section 1 of the full report and *Unintentional Insider Threats: Social Engineering*.

Findings

Our initial findings suggest that 19 out of 23 malware cases are multi-stage incidents. Of all 44 PHISHING/SOCIAL cases, only 15 were single-stage. These findings suggest multi-stage incidents are the norm across economic sectors. The only outliers of this trend are in the commercial and government facilities sectors, which showed increased occurrences of Credentials incidents. This could be due to higher levels of reporting requirements in these sectors.

Nothing in our research indicated that the mitigation strategies already outlined in previous research need to be updated. Current mitigations based on best practices described in our previous reports are still valid.

Recommendations

The research results to this point are limited by the small sample size of cases available. As our case collection grows, we can better determine the validity of the initial findings of the research. To advance the current practice and state of the art in computer and network defense, especially safeguards against phishing and other social engineering attacks, organizations should prepare and test their ability to prevent, detect, and respond to the incidents covered in this report by following

- the best practices in the *Common Sense Guide to Mitigating Insider Threats, 4th Edition*[4]
- the mitigation strategies outlined in the *Unintentional Insider Threats: A Foundational Study*

To help the research community determine the level and means of prevention and mitigation for this kind of threat, the following research needs should be addressed across the cyber community:

- Develop an extensive, confidential, self-reporting UIT database. The database should track the security equivalent of near-miss incidents tracked by many healthcare and manufacturing organizations. A UIT database could be used to track the quality of security at an organization over time and better assess the potential impact of a malicious insider attack.
- Perform more detailed analysis of UIT credentials and malware incidents and near incidents to inform the development of more effective mitigation approaches and tools.

[4] Silowash, George; Cappelli, Dawn; Moore, Andrew; Trzeciak, Randall; Shimeall, Timothy; & Flynn, Lori. *Common Sense Guide to Mitigating Insider Threats, 4th Edition* (CMU/SEI-2012-TR-012). Software Engineering Institute, Carnegie Mellon University, 2012. http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=34017

Abstract

The research documented in this report seeks to advance the understanding of the unintentional insider threat (UIT) that results from phishing and other social engineering cases, specifically those involving malicious software (malware). The research team collected and analyzed publicly reported phishing cases involving malware and performed an initial analysis of the industry sectors impacted by this type of incident. This report provides that analysis as well as case examples and potential recommendations for mitigating UITs stemming from phishing and other social engineering incidents. The report also compares security offices' current practice of UIT monitoring to the current manufacturing and healthcare industries' practice of tracking near misses of adverse events.

Introduction

Within government agencies, the second highest threat perceived by IT professionals is that of careless and untrained insiders. In a survey published by cybersecurity consultancy Solar Winds, 42% of respondents noted that insiders may inadvertently pose nearly as many risks to their agency as deliberate, malicious hackers [Solar Winds 2014]. This research supports the conclusions in the *Verizon Data Breach Report 2013* that 47% of malware was downloaded through e-mail attachments, 48% of hacking took place with stolen credentials, 77% of social engineering takes places through phishing, and 79% of social engineering takes place through e-mails [Verizon 2013]. Symantec's *Internet Security Threat Report 2014* revealed that the trends in this space are working against organizations: there has been a 91% increase in targeted e-mail attacks from 2012 to 2013, attackers are conducting longer campaigns,[1] and they are sometimes even following up these phishing attacks with phone calls to convince the unintentional insider to take immediate action without the opportunity to contemplate the risk involved [Symantec 2014]. The same report notes that the government (all levels) is the sector of the economy most frequently attacked by spear phishing, at 16% of all attacks in this space.

Two previous reports by the CERT® Insider Threat team, part of Carnegie Mellon University's Software Engineering Institute, provided an initial examination of the problem of unintentional insider threat (UIT) [CERT 2013] as well as how this problem is influenced by social engineering [CERT 2014]. The first of those reports characterized the UIT by developing an operational definition, reviewing relevant research to gain a better understanding of possible causes and contributing factors,[2] and providing examples of UIT cases and the frequencies of UIT occurrences across several categories. The second report, building off of the first, looked into social engineering and how the unintentional insider can be manipulated into acting against the organization's interest. These reports also documented an initial design of a UIT feature model, suggested mitigation strategies, and outlined incident paths for UIT-HACK incidents.

One challenge in researching the UIT problem and developing effective mitigation strategies is that the UIT topic and related incidents have gone mostly unreported. In particular, incident reports typically lack sufficient detail to inform analyses of potential contributing factors. The CERT Insider Threat team intended for our initial work on UIT cases [CERT 2013] to inform government and industry stakeholders about the problem and its potential causes and to guide research and development investments toward the highest priorities for countering UIT. Our second report published on this topic sought to advance our understanding of UIT contributing factors by focusing on a major type of UIT incident, social engineering [CERT 2014]. The goals of this re-

[1] "An attack campaign is defined as a series of emails that: A.) Show clear evidence that the subject and target has been deliberately selected. B.) Contain at least 3 or 4 strong correlations to other emails such as the topic, sender address, recipient domain, source IP C.) Are sent on the same day or across multiple days" [Symantec 2014].

® CERT® is a registered mark owned by Carnegie Mellon University.

[2] A *factor* is a situational element or feature that may or may not be related to the existence of the incident. A *contributing factor* is a factor that has been demonstrated to be associated as a causal factor of an incident. Because our research generally has not shown causal relationships, our usage of the term *contributing factor* should be interpreted as *potential contributing factor*.

search project were to collect additional UIT incident data, build them into a set of social engineering cases, and add that set to the CERT Division's Management and Education of the Risk of Insider Threat (MERIT) database (referred to as the *insider threat database*). Another goal was to analyze UIT cases to identify possible behavioral and technical patterns and precursors, with a particular focus on UIT cases that involve social engineering, to inform future research and development of UIT mitigation strategies.

This report focuses on the newly identified PHISHING/SOCIAL threat vector and its subvectors, Malware and Credentials. These threat vectors are influenced by the previous study on social engineering [CERT 2014]. The intent of this report is to identify the frequency of incident types (single-stage or multi-stage) that occur in different economic sectors within the United States. This research is based on the sample of incident cases the team has been able to collect from publicly available sources, which is often limited because organizations are reluctant to report incidents related to UIT. Due to limited amounts of information, we are unable to show a statistically significant difference between the types of incidents across industry sectors. Instead, we provide an overview of the cases that we have found as a general description of publicly reported UIT incidents.

The remainder of the report is organized as follows:

- Section 1, Defining and Characterizing the PHISHING/SOCIAL Threat Vector. This section updates the definition of the UIT-HACK threat vector to the Malware subvector.
- Section 2, Summary of Collected Cases. This section describes the data collection process that guides our collection and reporting of PHISHING/SOCIAL cases. This section also provides examples of representative cases.
- Section 3, Cases by Economic Sector. This section discusses results synthesized from research and case study analyses to identify patterns of frequent threat vectors within different economic sectors.
- Section 4, Initial Findings, and Section 5, Recommendations. Some of the recommendations come from adapting the reporting and tracking of near-miss events in healthcare and manufacturing organizations to a security context.

1 Defining and Characterizing the PHISHING/SOCIAL Threat Vector

1.1 Definition of UIT

Our initial research produced a working definition of an unintentional insider threat: "An unintentional insider threat is (1) a current or former employee, contractor, or business partner (2) who has or had authorized access to an organization's network, system, or data and who, (3) through action or inaction without malicious intent,[3] (4) causes harm or substantially increases the probability of future serious harm to the confidentiality, integrity, or availability of the organization's information or information systems" [CERT 2013]. In our second round of research, on social engineering, we recognized a need to modify the original definition slightly [CERT 2014]. One change was to emphasize that the unintentional insider's actions occur largely without the insider's knowledge or understanding of their impact, so we added the term "*unwittingly*"[4] to the fourth part of the definition. A second change was to modify the description of the target of the incident to include assets other than the organization's information system, such as financial systems. The report on the second round of research revised the definition as follows:

> *An unintentional insider threat is (1) a current or former employee, contractor, or business partner (2) who has or had authorized access to an organization's network, system, or data and who, (3) through action or inaction without malicious intent, (4) unwittingly causes harm or substantially increases the probability of future serious harm to the confidentiality, integrity, or availability of the organization's resources or assets, including information, information systems, or financial systems.*

1.2 Defining and Characterizing the New PHISHING/SOCIAL Threat Vector

In our previous work, we defined the UIT-HACK threat vector as

> *An outsider's electronic entry acquired through social engineering (e.g., phishing email incident, planted or unauthorized USB drive) and carried out via software, such as malware and spyware.*

Through further research, we have determined that many incidents initiated through phishing and other social engineering are not carried out by using software, but by acquiring and misusing the victim's credentials to secured systems. Because the common element of the two types of attacks is phishing and other social engineering, we created a new, larger category of threat vector, PHISHING/SOCIAL, that subsumes UIT-HACK, renames it as the subvector Malware, and adds the new subvector of Credentials:

[3] Malicious intent includes the intention to cause harm. Harm can also be caused by those who have no malicious intent (i.e., are nonmalicious), either by action or inaction, even if they knowingly break a rule (e.g., the guard who does not check badges does not mean to allow a malicious actor into the building, but he lets someone in who sets the building on fire.)

[4] This definition uses the perspective of the unintentional insider, which differs from the broader definition of social engineering acts that includes the (malicious and/or intentional) perpetrator's perspective.

- Malware (formerly UIT-HACK): *An outsider's electronic entry acquired through social engineering (e.g., phishing email incident, planted or unauthorized USB drive) and carried out via software, such as malware and spyware.*
- Credentials: *An outsider's electronic entry acquired through social engineering (e.g., phishing email incident) and carried out through compromised credentials, including passwords and other identifying information.*

The identification of the new threat subvector, Credentials, and the refinement of UIT-HACK allows researchers and those in operations to quickly differentiate the two types of incidents and take the most appropriate mitigation actions.

1.3 Single-Stage Incident

The incident progression for a single-stage incident generally comprises five steps, as shown in Figure 1. We used this variation of the kill-chain model, well known across the computer security industry, as a foundation and customized the delivery, exploitation, and command-and-control steps to accommodate the specifics of social engineering. The steps shown in Figure 1 represent general building blocks on which more complicated incidents (multi-stage) may be based. Each phase of the incident has different objectives that can change opportunistically depending on what information is captured during the social engineering operation. The general workflow pattern of typical actions taken by an outsider allows for this flexibility.

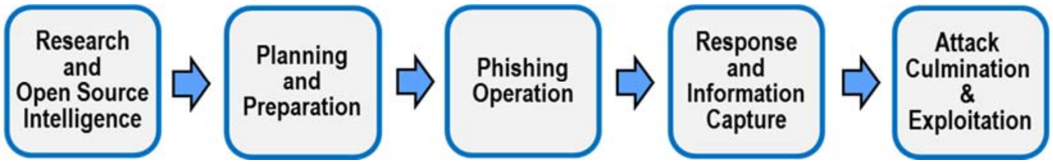

Research and Open Source Intelligence
Planning and Preparation
Phishing Operation
Response and Information Capture
Attack Culmination & Exploitation

Figure 1: Workflow Pattern Showing Phases of a Single-Stage Phishing Incident

In the first phase, the attacker researches possible targets. Based on information gathered, the second phase, Planning and Preparation, progresses by the attacker preparing phishing artifacts. The attacker then executes the phishing operation by sending phishing emails to recipients in the target organization. Many recipients do not respond, but those who do respond may become a UIT. In the Response and Information Capture phase, the UIT unwittingly sends account information to the attacker's system. After the information is received, the attacker conducts the final phase of the incident by using the account credentials to gain access to the unwitting individual's machine and plant malware or take other measures directed against the organization. Table 1 shows typical actions that characterize each phase of the phishing incident.

Figure 2 shows a use-case model of the single-stage incident.

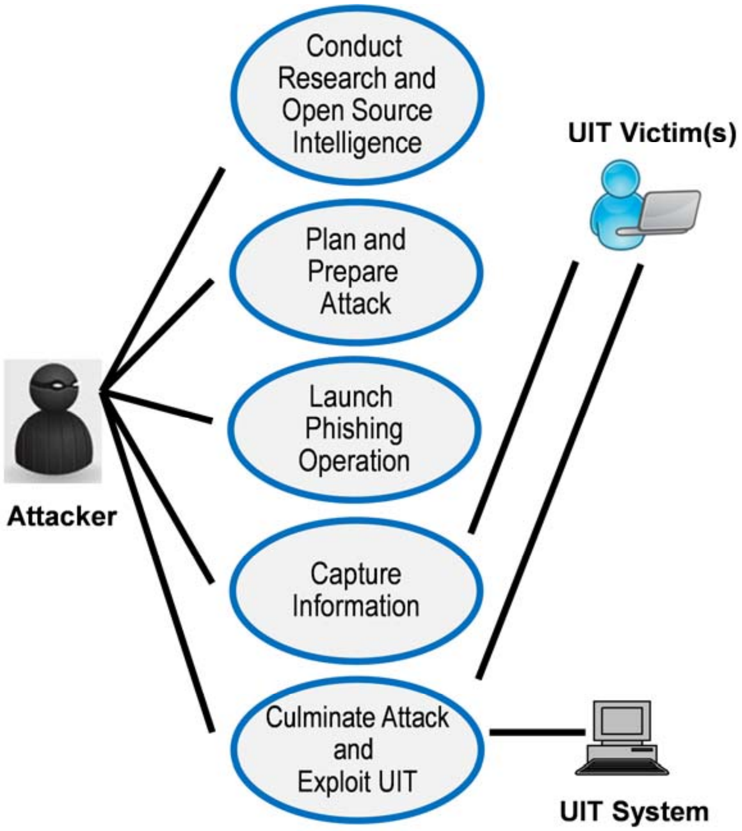

Conduct Research and Open Source Intelligence
Plan and Prepare Attack
Launch Phishing Operation
Capture Information
Culminate Attack and Exploit UIT
UIT Victim(s)
Attacker
UIT System

Figure 2: Use-Case Model for Single-Stage Social Engineering Incident

Table 1: Steps in a Single-Stage Phishing Malware Incident

Pattern Phase	Typical Activities	Pattern Interactions
1. Research and Open Source Intelligence	• Search for open source intelligence • Establish incident objectives • Identify opportune targets	1.1 Attacker researches and strategizes about potential targets and specific objectives.
2. Planning and Preparation	• Develop incident strategy including means to avoid detection and mitigation by UIT organization • Prepare phishing incident artifacts	2.1 Attacker plans phishing incident and creates phishing artifacts (e.g., phishing email, mobile text message, phony website, malware to be implanted).
3. Phishing Operation	• Release phishing artifact via email, cell phone, rogue website, or other means • Wait for a response	3.1 Attacker initiates phishing incident through email, cell phone, rogue website, or other means.
4. Response and Information Capture	• Gain access and/or privileges to obtain greater information reach • Implant malware to achieve information objectives • Identify other opportune UIT targets and internal system information, and capture guarded and sensitive information	4.1 One or more targets unwittingly responds to phishing artifact and becomes a UIT. 4.2 Attacker detects or is alerted to UIT response and obtains initial information directly from UIT data entry. 4.3 Attacker implants malware on victim's machine or network. 4.4 Attacker obtains desired information via malware.
5. Incident Culmination & Exploitation	• Use captured information to directly influence UIT or UIT's organization to steal, manipulate, and/or destroy targeted assets	5.1 Attacker uses desired information in direct incident on UIT or UIT's organization to steal, manipulate, and/or destroy targeted assets.

Figure 3 shows a class model for a social engineering incident. The human participants in the Attack Participant class include the attacker and some number of UIT victims. In many phishing incidents, the attacker directs email messages to a large number of potential UITs, or the potential UITs visit phishing websites. Only those who take the bait fall into the UIT Victim(s) subclass. The Attack Media class highlights the means that the attacker uses to obtain information, either through research in the early phases of the incident or via UIT responses, malware, or other electronic means. To carry out an exploit, attackers generate a variety of objects in the Attack Artifacts class, including email, malware, or web pages.

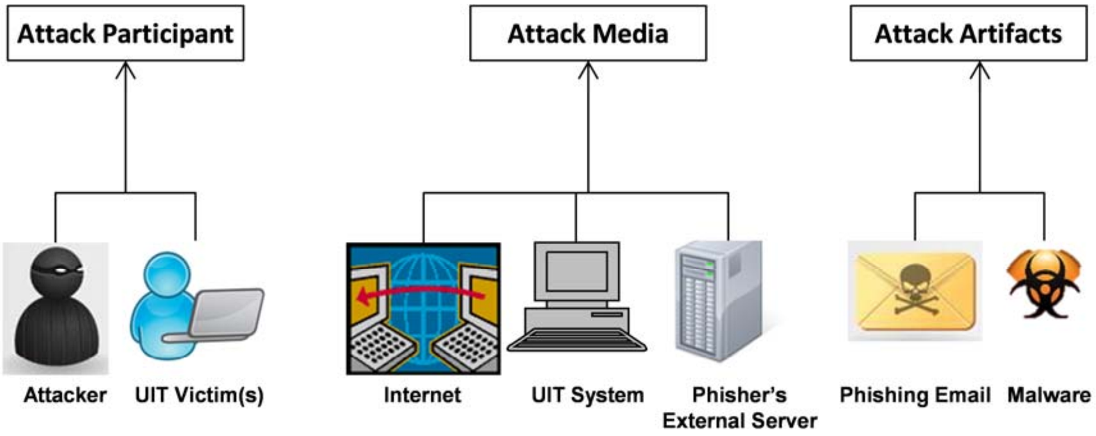


Figure 3: Incident Class Model for a Social Engineering Incident

Figure 4, a swim-lane chart, provides another perspective on the single-stage phishing incident. It shows the sequence of actions for the attacker and the victim(s).

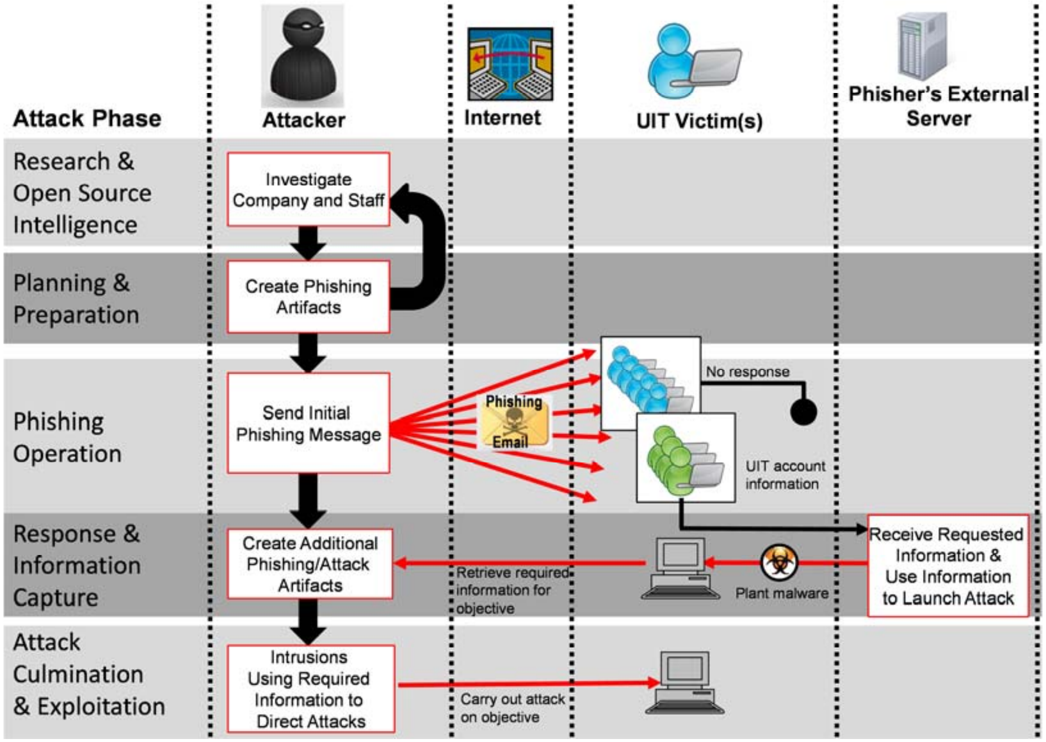

Attack Phase
Attacker
Internet
UIT Victim(s)
Phisher's External Server
Research & Open Source Intelligence
Investigate Company and Staff
Planning & Preparation
Create Phishing Artifacts
Phishing Operation
Send Initial Phishing Message
Phishing Email
No response
UIT account information
Response & Information Capture
Create Additional Phishing/Attack Artifacts
Retrieve required information for objective
Plant malware
Receive Requested Information & Use Information to Launch Attack
Attack Culmination & Exploitation
Intrusions Using Required Information to Direct Attacks
Carry out attack on objective

Figure 4: Swim-Lane Chart of Actions Taken by Attacker and UIT Victims in a Single-Stage Incident

Finally, the interaction view (Figure 5) peels the swim lanes apart to show each interaction and the exchanges that occur to carry out an incident. This view illustrates the collaborations of each element of the swim-lane view for a single-phase incident. The sequence of interactions shows the information exchanges during each phase of the incident.

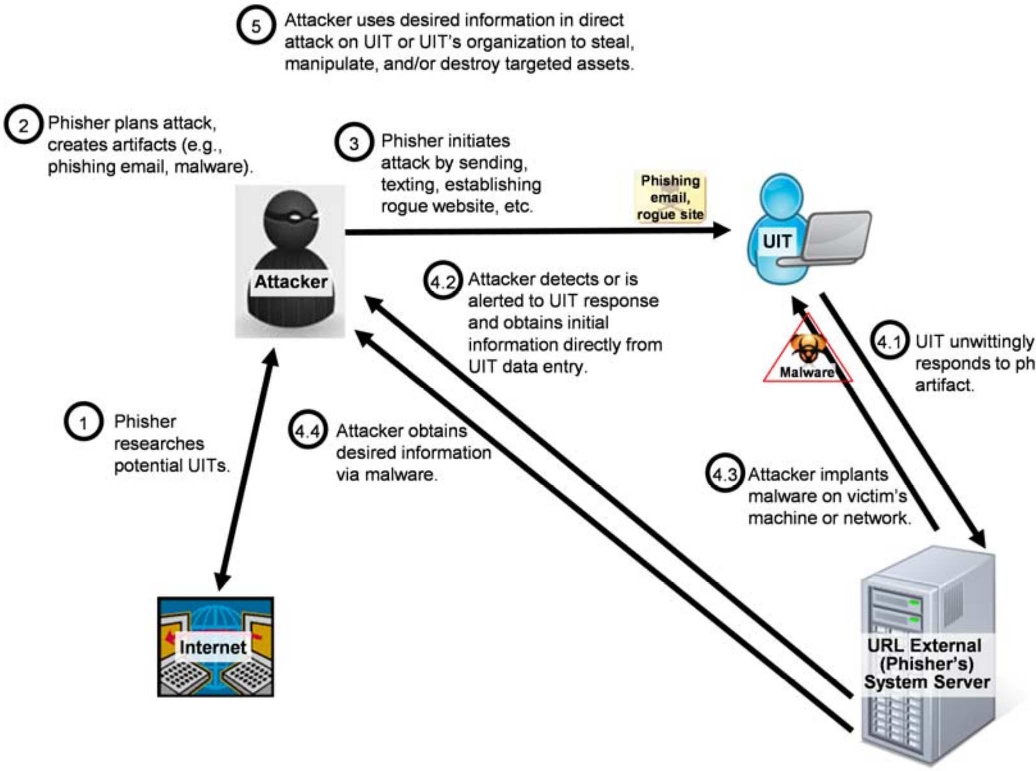

5 Attacker uses desired information in direct attack on UIT or UIT's organization to steal, manipulate, and/or destroy targeted assets.
2 Phisher plans attack, creates artifacts (e.g., phishing email, malware).
3 Phisher initiates attack by sending, texting, establishing rogue website, etc.
Phishing email, rogue site
UIT
Attacker
4.2 Attacker detects or is alerted to UIT response and obtains initial information directly from UIT data entry.
4.1 UIT unwittingly responds to phishing artifact.
Malware
1 Phisher researches potential UITs.
4.4 Attacker obtains desired information via malware.
4.3 Attacker implants malware on victim's machine or network.
Internet
URL External (Phisher's) System Server

Figure 5: Interaction View Showing Object Collaboration in a Single-Stage Social Engineering Incident

1.4 Multi-Stage Incident

The multiple-stage incident follows a similar pattern to the single-stage incident, but once the attacker has UIT system access, the attacker identifies other potential UITs and subsequently directs social engineering at them. The attacker may also use the access gained to probe the UIT's system to gather intelligence about the compromised systems or networks, and use the information to cause harm or develop subsequent spear phishing messages. The workflow diagram in Figure 6 shows the multi-stage incident chain. This diagram identifies the ordering and decision processes involved in each phase of the exploit.

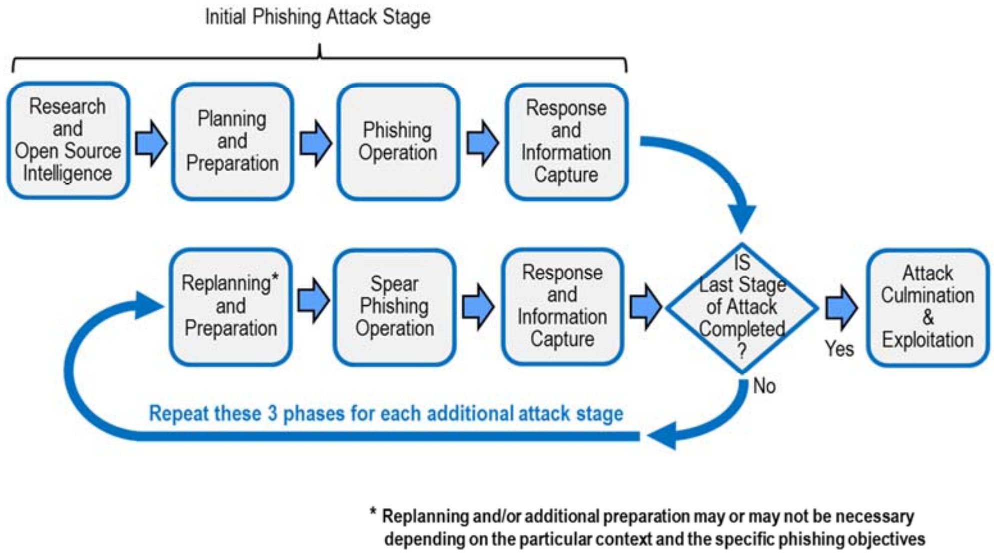

Initial Phishing Attack Stage
Research and Open Source Intelligence
Planning and Preparation
Phishing Operation
Response and Information Capture
Replanning* and Preparation
Spear Phishing Operation
Response and Information Capture
IS Last Stage of Attack Completed ?
Yes
No
Attack Culmination & Exploitation
Repeat these 3 phases for each additional attack stage
* Replanning and/or additional preparation may or may not be necessary depending on the particular context and the specific phishing objectives

Figure 6: Workflow Diagram Incident Chain for Multiple-Stage Phishing Exploit

Table 2 shows the steps or phases of a multiple-stage phishing incident. Steps 1–4 of the single-stage incident (Table 1) occur, but the multiple-stage incident includes additional iterative steps (shown in bold-face type in Table 2) that represent the repeated planning and preparation, (spear) phishing, and response and information capture operations prior to conducting the delayed incident.

Table 2: Steps in a Multiple-Stage Phishing Malware Incident

Pattern Phase	Typical Activities	Pattern Interactions
1. Research and Open Source Intelligence	• Search for open source intelligence • Establish incident objectives • Identify opportune targets	1.1 Attacker researches and strategizes about potential targets and specific objectives.
2. Planning and Preparation	• Develop incident strategy including means to avoid detection and mitigation by UIT organization • Prepare phishing incident artifacts	2.1 Attacker plans phishing incident and creates phishing artifacts (e.g., phishing email, mobile text message, phony website, malware to be implanted).
3. Phishing Operation	• Release phishing artifact via email, cell phone, rogue website, or other means • Wait for a response	3.1 Attacker initiates phishing incident through email, cell phone, rogue website, or other means.
4. Response and Information Capture	• Gain access and/or privileges to obtain greater information reach • Implant malware to achieve information objectives • Identify other opportune UIT targets and internal system information, and capture guarded and sensitive information	4.1 One or more targets unwittingly respond to phishing artifact and become a UIT. 4.2 Attacker detects or is alerted to UIT response and obtains initial information directly from UIT data entry. 4.3 Attacker implants malware on victim's machine or network. 4.4 Attacker obtains desired information via malware.
5. Re-planning and Preparation	• **Re-plan incident strategy including means to avoid detection and mitigation by UIT organization** • **Prepare spear phishing incident artifacts**	**5.1 Attacker uses information capture in step 4 to re-plan follow-on steps for spear phishing incident. This may entail creation of new artifacts or specific incident approaches.**
6. Spear Phishing Operation / Use Malicious Software to Traverse Network	• **Execute spear phishing** • **Wait for a response**	**6.1 Attacker initiates spear phishing incident.** **6.2 One or more high-value targets unwittingly responds to the spear phishing artifact and becomes a UIT.**
7. Response and Information Capture	• **Gain access and/or privileges to obtain greater information reach** • **Exploit specific insider targets: e.g., financial systems, secure systems, intellectual property, etc.**	**7.1 Malicious software is used to traverse the network.** **7.2 Phisher detects or is alerted to UIT response and obtains desired information directly from UIT data entry.**
8. Incident Culmination & Exploitation	• Use captured information to directly influence UIT or UIT's organization to steal, manipulate, and/or destroy targeted assets	8.1 Attacker uses desired information in direct incident on UIT or UIT's organization to steal, manipulate, and/or destroy targeted assets.

Figure 7 depicts the interaction view of object collaboration in the multiple-stage social engineering incident. The objects are derived from the single-stage incident's class model (Figure 3), but there are more instances of them.

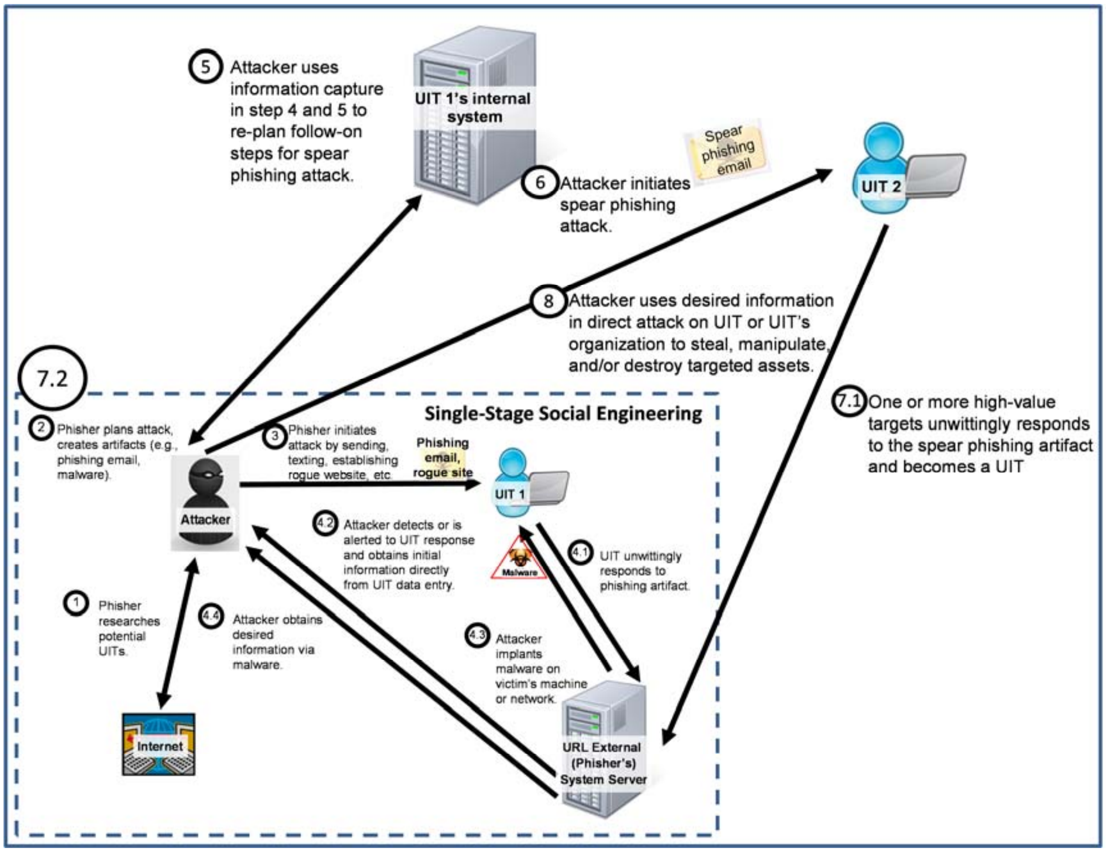

5 Attacker uses information capture in step 4 and 5 to re-plan follow-on steps for spear phishing attack.
UIT 1's internal system
Spear phishing email
6 Attacker initiates spear phishing attack.
UIT 2
8 Attacker uses desired information in direct attack on UIT or UIT's organization to steal, manipulate, and/or destroy targeted assets.
7.2
Single-Stage Social Engineering
7.1 One or more high-value targets unwittingly responds to the spear phishing artifact and becomes a UIT
2 Phisher plans attack, creates artifacts (e.g., phishing email, malware).
3 Phisher initiates attack by sending, texting, establishing rogue website, etc.
Phishing email, rogue site
UIT 1
Attacker
4.2 Attacker detects or is alerted to UIT response and obtains initial information directly from UIT data entry.
Malware
4.1 UIT unwittingly responds to phishing artifact.
1 Phisher researches potential UITs.
4.4 Attacker obtains desired information via malware.
4.3 Attacker implants malware on victim's machine or network.
Internet
URL External (Phisher's) System Server

Figure 7: Interaction View Showing Object Collaboration in a Multiple-Stage Social Engineering Incident

Figure 8 illustrates an actual incident used in the development of the UIT model, Case ID# 45, which represents a single-stage social engineering pattern. Figure 9 illustrates another incident, Case ID# 42, which represents a multiple-stage social engineering pattern, to show the similarities and differences between the two UIT types.

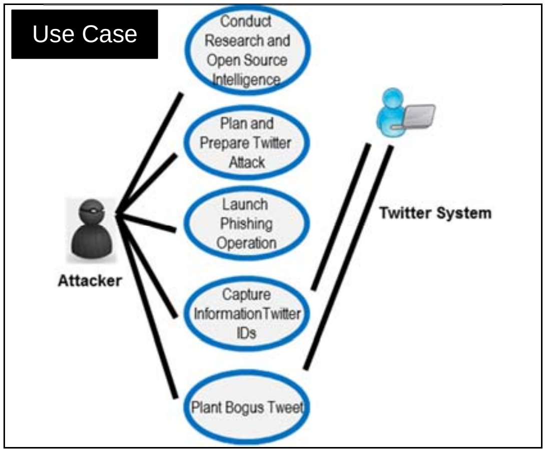
This following case provides an example of a multi-staged phishing attack that resulted in a UIT Hacking Malware case. The case involves the hacking of a major media source's Twitter feed via a phishing email that contained malware. Once the hackers had control of the Twitter feed, they tweeted a fake message regarding an attack on a major U.S. target. During the next three minutes, this caused a significant downward turn in the Dow Jones Industrial Average.

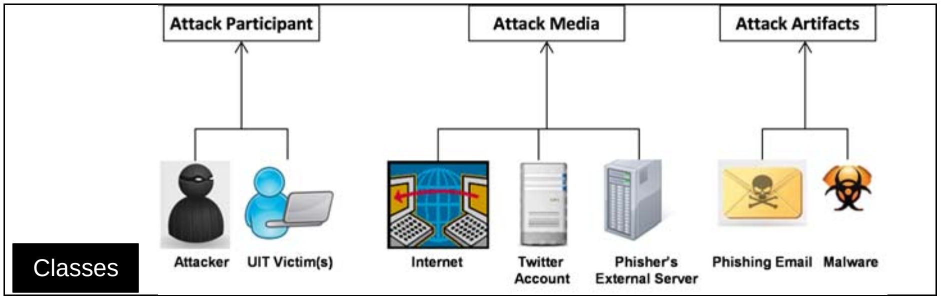
A company was phished with an email stating that their transactions hadn't cleared and were asked to click on a link to resolve the issue. Once the insider clicked on the link, a keylogger was installed on their computer which was used to steal password information for the agency that completed wire transfers for the company. The hackers requested that the wire transfer agency send money through another bank and to a bank in another country. The wire transfer company sent a confirmation email of the transfer to the company who called to cancel the transaction; however, it was too late.

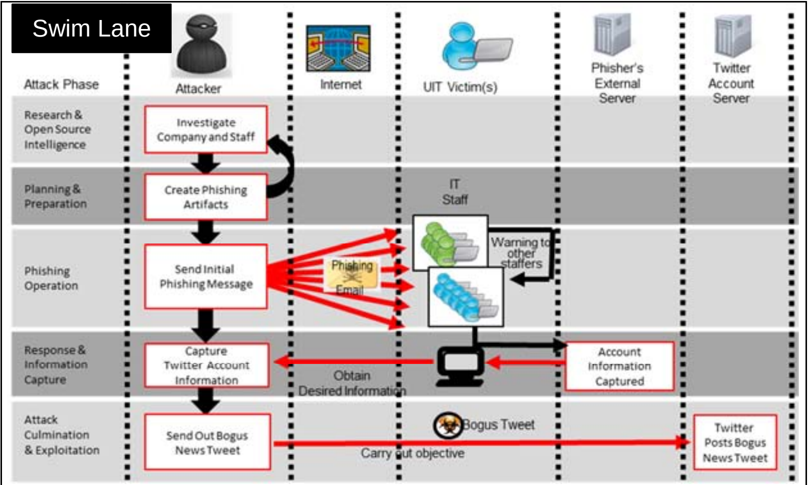
Example 1: Case #45

The incident is launched against a major news organization. A bogus news story is planted on the organization’s Twitter feed to disrupt financial markets.

Shown here are the use case (right), participant classes (upper right), swim lane activities (below), and collaboration model (far right).
Instead of malware, the attacker plants a bogus news feed. The final use case is extended to plant the news feed.


Use Case
Conduct Research and Open Source Intelligence
Plan and Prepare Twitter Attack
Launch Phishing Operation
Capture Information Twitter IDs
Plant Bogus Tweet
Attacker
Twitter System




Swim Lane
Attack Phase
Attacker
Internet
UIT Victim(s)
Phisher's External Server
Twitter Account Server
Research & Open Source Intelligence
Investigate Company and Staff
Planning & Preparation
Create Phishing Artifacts
IT Staff
Phishing Operation
Send Initial Phishing Message
Phishing Email
Warning to other staffers
Response & Information Capture
Capture Twitter Account Information
Obtain Desired Information
Account Information Captured
Attack Culmination & Exploitation
Send Out Bogus News Tweet
Bogus Tweet
Carry out objective
Twitter Posts Bogus News Tweet

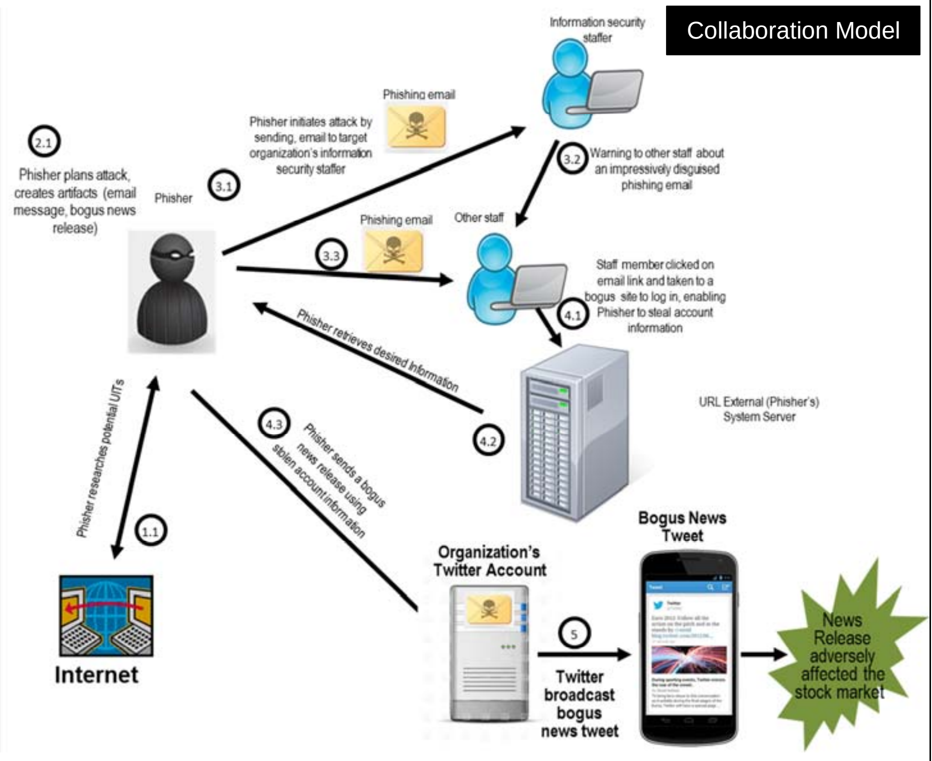

Collaboration Model
Information security staffer
Phishing email
Phisher initiates attack by sending, email to target organization's information security staffer
2.1
Phisher plans attack, creates artifacts (email message, bogus news release)
Phisher
3.1
3.2
Warning to other staff about an impressively disguised phishing email
Phishing email
Other staff
3.3
Staff member clicked on email link and taken to a bogus site to log in, enabling Phisher to steal account information
4.1
Phisher retrieves desired Information
4.2
URL External (Phisher's) System Server
Phisher researches potential UITs
4.3
Phisher sends a bogus news release using stolen account information
1.1
Internet
Organization's Twitter Account
5
Twitter broadcast bogus news tweet
Bogus News Tweet
News Release adversely affected the stock market

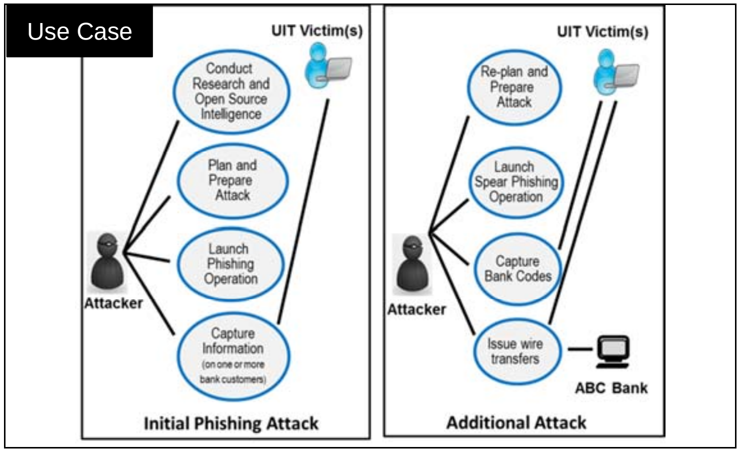
Figure 8: Illustration of Concepts and Patterns Applied to Case #45

In the collaboration model (above), the incident uses a phishing message (#3) against the organization’s staff to obtain account information (#4). With the account information, the incident is able to impersonate staff and plant the bogus news feed (#5).

Example 2: Case # 42

The incident is launched against companies using wire transfers. The target is a funds transfer account with any company using wire transfers with a specific bank. The attacker phishes the bank's customers, and ABC responds. The spear phishing goes to ABC with the intent of capturing ABC's wire transfer authorization codes, using them to perform a series of transfers from ABC's account to accounts held by the attacker in off-shore banks.

Shown here are use cases, participant classes, and swim-lane activities. The second stage is not completely illustrated in the swim-lane graphic. After an initial set of phishing messages and receipt of a response from ABC, the attacker sends a spear phishing message to ABC to obtain wire transfer codes.


Use Case
UIT Victim(s)
Conduct Research and Open Source Intelligence
Plan and Prepare Attack
Launch Phishing Operation
Capture Information (on one or more bank customers)
Attacker
Initial Phishing Attack
UIT Victim(s)
Re-plan and Prepare Attack
Launch Spear Phishing Operation
Capture Bank Codes
Issue wire transfers
Attacker
ABC Bank
Additional Attack

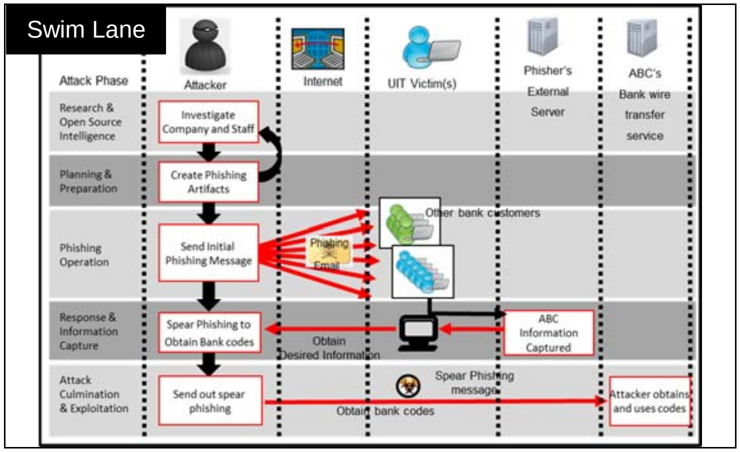
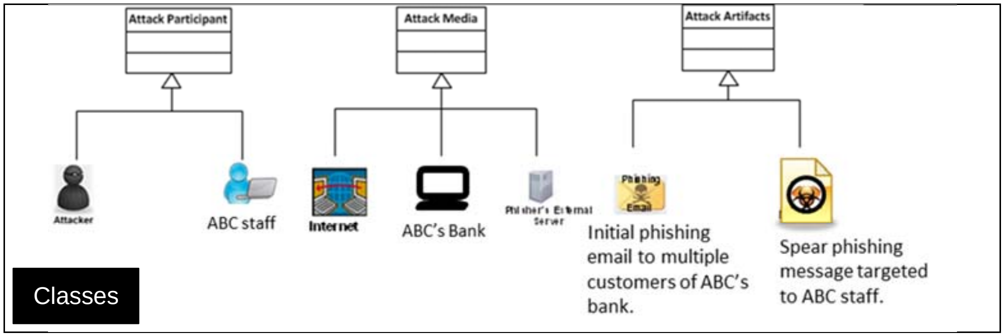
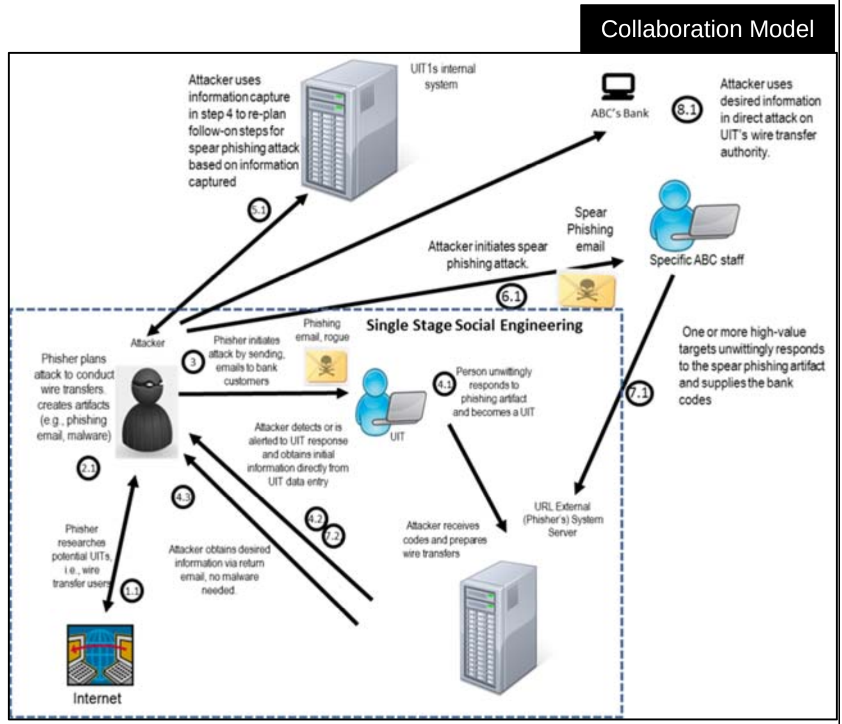

Swim Lane
Attack Phase
Attacker
Internet
UIT Victim(s)
Phisher's External Server
ABC's Bank wire transfer service
Research & Open Source Intelligence
Investigate Company and Staff
Planning & Preparation
Create Phishing Artifacts
Phishing Operation
Send Initial Phishing Message
Phishing Email
Other bank customers
Response & Information Capture
Spear Phishing to Obtain Bank codes
Obtain Desired Information
ABC Information Captured
Attack Culmination & Exploitation
Send out spear phishing
Spear Phishing message
Obtain bank codes
Attacker obtains and uses codes

Figure 9: Illustration of Concepts and Patterns Applied to Case #42


Attack Participant
Attack Media
Attack Artifacts
Attacker
ABC staff
Internet
ABC's Bank
Phisher's External Server
Phishing Email
Initial phishing email to multiple customers of ABC's bank.
Spear phishing message targeted to ABC staff.
Classes

In the collaboration model, the incident uses a phishing message (#3) against bank customers. When ABC responds (#4.1, #4.2), it becomes the target of spear phishing to obtain the codes (#6.1, #7.1). With the account information, the attacker is able to impersonate ABC and perform the transfers. (#8.1)


Collaboration Model
Attacker uses information capture in step 4 to re-plan follow-on steps for spear phishing attack based on information captured
UIT1s internal system
ABC's Bank
8.1
Attacker uses desired information in direct attack on UIT's wire transfer authority.
5.1
Spear Phishing email
Attacker initiates spear phishing attack.
Specific ABC staff
6.1
Attacker
Phishing email, rogue
Single Stage Social Engineering
Phisher plans attack to conduct wire transfers. creates artifacts (e.g., phishing email, malware)
3
Phisher initiates attack by sending, emails to bank customers
4.1
Person unwittingly responds to phishing artifact and becomes a UIT
UIT
One or more high-value targets unwittingly responds to the spear phishing artifact and supplies the bank codes
7.1
2.1
Attacker detects or is alerted to UIT response and obtains initial information directly from UIT data entry
4.3
4.2
7.2
Attacker receives codes and prepares wire transfers
URL External (Phisher's) System Server
Phisher researches potential UITs, i.e., wire transfer users
1.1
Attacker obtains desired information via return email, no malware needed.
Internet

2 Summary of Collected Cases

Case study research is not a valid method for making generalizable inferences. Yet without case studies, researchers are left to infer what factors and parameters are important. Collecting and analyzing PHISHING/SOCIAL and Malware case studies is helpful for identifying factors and relationships that may be addressed later in experimental and observational research, enabling statistical testing of hypothesized relationships (e.g., causal, correlational, moderating, mediating, predictive) between factors and incidents. By informing experimental and observational research, case study research improves the validity and generalizability of these hypothesized relationships. Table 3 shows the attributes from UIT cases that we recorded for this study.

Table 3: Recorded Attributes of UIT Cases

Attribute	Definition
Incident ID	Unique identifier for each case
Incident Type	Single- or multi-stage
Victim Organization Industry Sector	Critical infrastructure sector
Summary and Description of Attack Vector	Summary of incident
Classified Data	Was classified data exposed?
Encrypted Data	Was the exposed data encrypted?
Spear Phishing	Was spear phishing used?
Type of Incident	PHISHING/SOCIAL and/or Malware

We use these parameters to summarize representative examples of incidents in the following section.

2.1 Representative Cases

In this section, selected UIT social engineering incidents are described, using a variation of the incident template in Table 3. The case information comes from

- reports, captured during previous research by the team, that fall into the PHISHING/SOCIAL and Malware categories
- news reports captured through internet searches using search strings to locate relevant incidents

For ease of presentation and to help describe patterns, the cases are categorized into single- or multiple-stage incidents. This categorization reflects our observation, based on examining cases collected, that many of the incidents may be decomposed into separate stages that share common characteristics of incident evolution.

2.1.1 PHISHING/SOCIAL

2.1.1.1 Single-Stage PHISHING/SOCIAL Incidents

Sample 1

Incident ID 62

INDUSTRY: Healthcare/Public Health

STAGING: Single

INCIDENT: A doctor at a healthcare provider was spear phished by hackers purporting to be from the company's IT department. The doctor provided his credentials, which potentially allowed the hackers to access personal information regarding patients, including their demographic and clinical data.

Stage 1 - phishing a doctor

IMPACT: Potential access to personal information such as demographic and clinical data.

OUTCOME: Unknown

RESPONSE: The healthcare organization notified the patients that their personal information may have been breached.

2.1.1.2 Multiple-Stage Phishing Incidents

Sample 1

Incident ID 48

INDUSTRY: Commercial facilities

STAGING: Multiple

INCIDENT: A group of political hackers directed a targeted phishing attack against employees at an online publication. The attack was successful and allowed the hackers to gain access to employee emails, send out emails purporting to be from coworkers who were phished, and ultimately gain access to the company's Twitter account, allowing for the attackers to post their political views from the publication's Twitter feed.

Stage 1 – several-staged phishing attack of employees

Stage 2 – phishing from stage 1 allowed access to social media site through compromised credentials

BREACH: Several multi-staged phishing attacks allowed for phishers to gain access to company's social media site and post political messages to a broad online audience.

OUTCOME: Company regained control of its social media site.

RESPONSE: All company users were asked to change their passwords. Company tech team put out memorandum outlining recommendations for how other companies could avoid similar attacks.

2.1.2 Malware

2.1.2.1 Single-Stage Malware

Sample 1

Incident ID 56

INDUSTRY: Healthcare/Public Health

STAGING: Single

INCIDENT: Email accounts of several healthcare employees were compromised by phishing attack. This attack led to the compromise of 1,800 patients' personal health information (PHI). This information included medical visit information but, fortunately, did not include credit card or Social Security numbers. The breach came to light when the email accounts of these employees were subsequently deleted. In addition, these employees' email accounts were utilized to send emails to others outside of their healthcare system. The company reported that similar phishing emails were deleted from other employees' accounts and that the phishing site was blocked by the IT department.

BREACH: PHI was released.

OUTCOME: Emails were encrypted, but it is unknown if hackers gained access to PHI.

RESPONSE: The phishing emails were deleted from other staff accounts, employees were warned about the scam, and employee access to the phishing site was blocked.

Hijacking of social networking accounts has become more common, and social media (e.g., Facebook, LinkedIn) are frequent targets of cyber incidents. In addition to offering access to various systems and accounts, they provide background used as intelligence to support the initial phishing. The news organization affected by this specific incident had intended to use Twitter for newsgathering and to combat rumors, but Twitter's security weakness makes it a prime target. The need for hot-list items and other immediate news information may cause otherwise security-conscious users to relax their guards.

2.1.2.2 Multi-Stage Malware

Incident ID 34

INCIDENT ID: 34

INDUSTRY: Government facilities

STAGING: Multi

INCIDENT: An employee fell prey to a spear phishing email that was malware infested. The employee opened the malicious email, which allowed hackers to steal the employee's username and password. This allowed attackers to access a significant amount of sensitive, personal data over a period of several months. Several weeks later, the hackers used these credentials to gain remote access to the company's site and that employee's computer. From this point, the attackers pivoted onto other systems and databases and exfiltrated approximately 8.2 GB of data.

BREACH: Accessing an employee account via a malicious spear phishing email allowed phishers access to computer systems that contained the Social Security numbers of millions of people. Two-factor authentication, which allowed access into the systems that contained the personal information, was not in place, nor was the sensitive personal data of employees encrypted. It is unknown what occurred with the exfiltrated data.

OUTCOME: Unknown

RESPONSE: The company issued a statement that they had implemented new technologies that aimed to address previous security issues. They also offered identity protection coverage.

3 Cases by Economic Sector

3.1 Case Studies, Characteristics, and Patterns of Threat Vector by Economic Sector

This section describes the process we used to categorize the incidents and identify the victim organization's sector, and it describes patterns of the UIT incidents specific to economic sectors.

3.1.1 PHISHING/SOCIAL Threat Vector by Economic Sector

Within the CERT Insider Threat Center's 110-case UIT corpus, the PHISHING/SOCIAL threat vector accounts for 44. These cases break down by economic sector of the United States as shown in Figure 10:

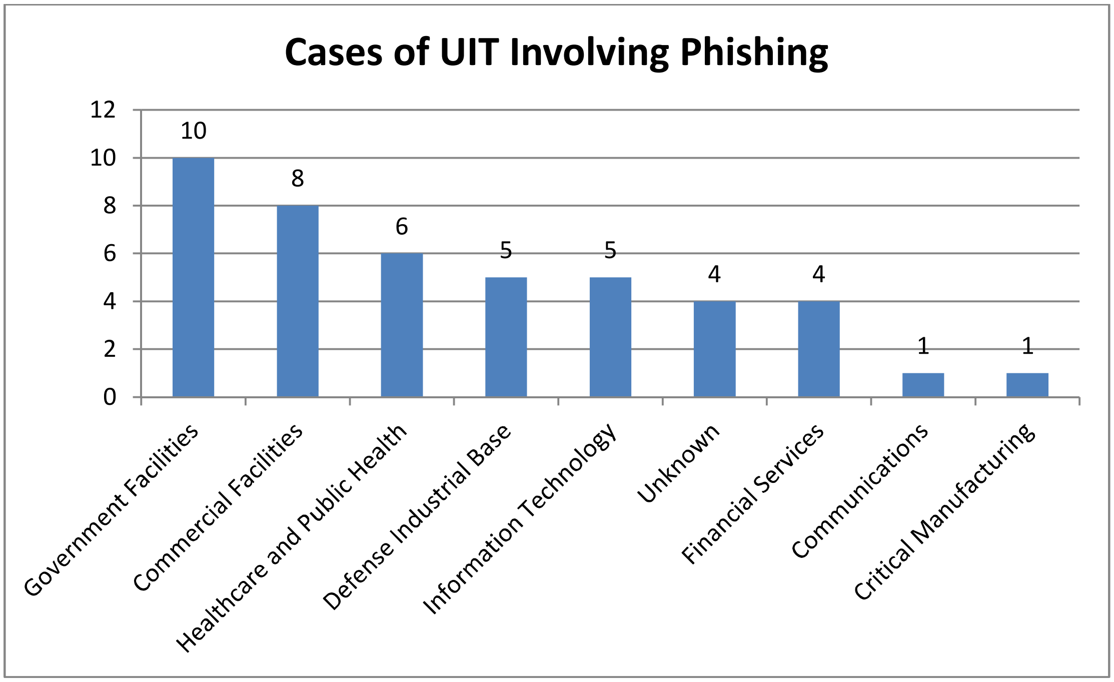


Figure 10: Cases of UIT Involving Phishing by Economic Sector

3.1.2 Malware Threat Subvector by Economic Sector

The Malware subvector offers a compelling area of research because of the high stakes this kind of incident entails. Organizations experiencing this kind of incident will mitigate it differently than they would if only the loss of credentials was at stake, as experienced in the Credentials threat subvector. Malware incidents constitute 43% of PHISHING/SOCIAL cases in our database, or 23 out of 44. These cases break down by economic sector of the United States as shown in Figure 11:

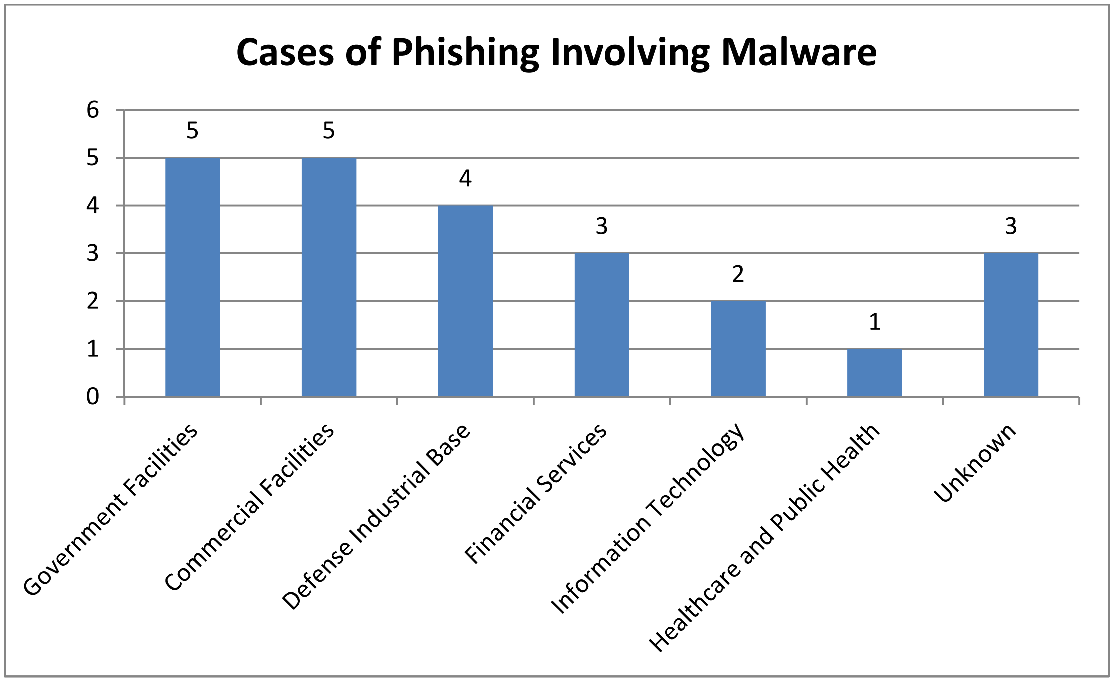


Figure 11: Cases of UIT Involving Malware by Economic Sector

3.2 Case Studies, Characteristics, and Patterns of Threat Vector by Economic Sector

Our initial findings suggest that most Malware cases are multi-staged, while most Credentials cases are single-stage. Of the 23 Malware cases, 19 were multi-stage. Of all 44 PHISHING/SOCIAL cases, 15 were single-stage.

4 Initial Findings

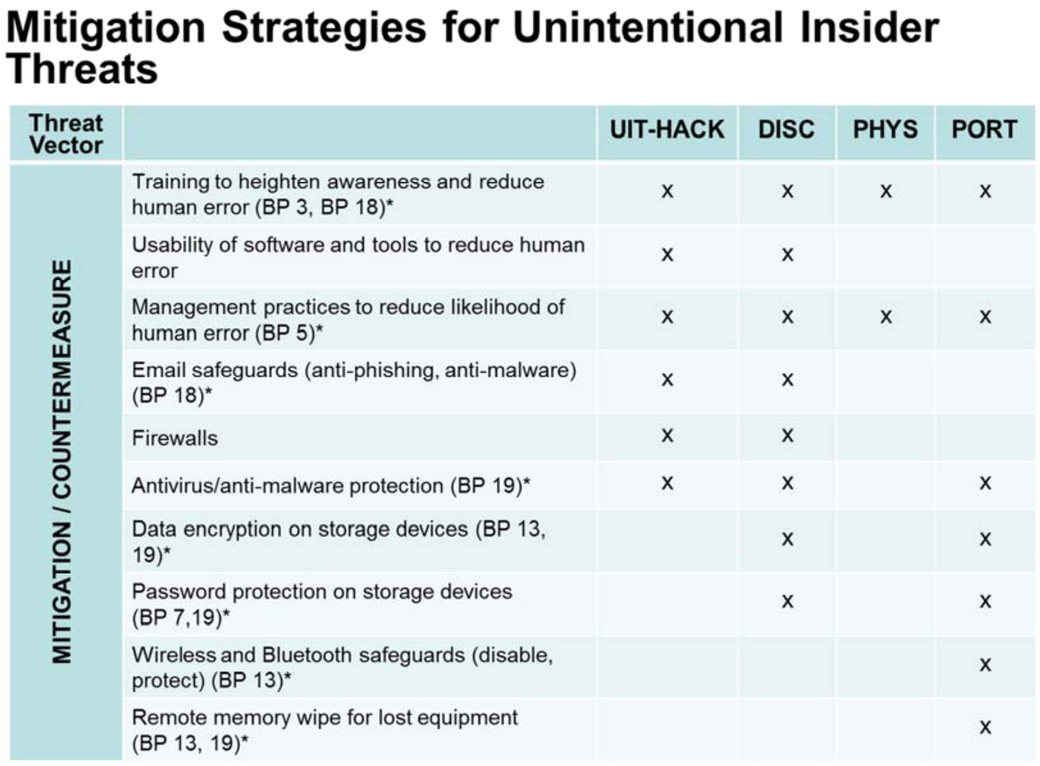
4.1 Findings

Our initial findings suggest that multi-stage and single-stage incidents are almost evenly spread across all sectors of the U.S. economy. The only outliers of this trend are in the commercial and government facilities sectors, which showed increased occurrences of single-stage PHISHING/SOCIAL incidents. However, this could be due to higher levels of reporting requirements in these sectors.

Inferring from the results cited, the team concludes that there is a possible trend in single-stage incidents leading toward outside malicious actor ownership of an organization’s social media presence, while multi-stage incidents are geared more toward the introduction of malware.

These findings are not definitive, nor should they be taken as a call to action. They are based on a very limited sample set, within a community that lacks proper reporting mechanisms, requirements to report, or places in which to share this information.

Nothing in our research signaled that the mitigation strategies already outlined in previous research needs to be updated [CERT 2013]. In fact, the mitigation strategies outlined in the UIT foundational study, as can be seen in Figure 12, are still valid.



Mitigation Strategies for Unintentional Insider Threats

Threat Vector		UIT-HACK	DISC	PHYS	PORT
MITIGATION / COUNTERMEASURE	Training to heighten awareness and reduce human error (BP 3, BP 18)*	x	x	x	x
	Usability of software and tools to reduce human error	x	x		
	Management practices to reduce likelihood of human error (BP 5)*	x	x	x	x
	Email safeguards (anti-phishing, anti-malware) (BP 18)*	x	x		
	Firewalls	x	x		
	Antivirus/anti-malware protection (BP 19)*	x	x		x
	Data encryption on storage devices (BP 13, 19)*		x		x
	Password protection on storage devices (BP 7,19)*		x		x
	Wireless and Bluetooth safeguards (disable, protect) (BP 13)*				x
	Remote memory wipe for lost equipment (BP 13, 19)*				x

Figure 12: UIT Foundational Study’s Mitigation Strategies

Reviewing the recommendations provided in the UIT foundational study [CERT 2013], we have confirmed that these mitigation strategies apply to Malware incidents. Our research confirms that the strategies presented in the foundational study may have been useful, in each of the cases we analyzed, for preventing, detecting, or responding to such events.

As noted in the foundational study, a proactive approach to creating a healthy and productive work environment is an essential first step in managing UITs. These steps involve practices that aim to avoid workload pressure and overworked staff, thereby decreasing the propensity for staff to fall prey to phishing emails or other socially engineered attacks. Furthermore, it is essential to provide adequate education to staff regarding methods used by adversaries to use insiders to unwittingly harm the organization (from the foundational study, Best Practice (BP) 3, BP 18). This education enables staff to recognize social media and phishing threats appropriately. Approximately 40% of the UIT cases we analyzed deal with phishing attacks, and 52% of those progressed to Malware cases. Employment of proper mitigation strategies might have prevented these cases.

The protection of the network is also a key general protection strategy. Employees who are educated on the threat vectors may be less likely to click on a potentially malicious link or attachment in an email that may be malware-laced, thus protecting the network. Companies are encouraged to put in place anti-malware and anti-phishing software to proactively address potential threats (BP 19). The use of firewalls is also strongly encouraged. Maintaining data encryption (BP 13, 19) on storage devices as well as password protection for individual users (BP 7, 19) could mitigate phishing attacks leading to hacks that involve data exfiltration.

4.1.1 Near Misses and Understanding and the Potential Impact of an Insider Attack

The appropriate value to invest in insider threat mitigation is unique to all organizations. The expected cost of an insider threat attack to an organization can be viewed as the estimated cost of an insider attack multiplied by the probability that an attack will occur. To accurately identify the potential cost of an attack, organizations must prioritize their critical assets and know the exposure of their critical assets to insiders. The exposure of critical assets to insiders represents the potential for an insider attack. The higher the potential for an attack, the greater the probability of an attack. The organization can calculate their risk exposure from insider threats by multiplying the probability of an insider attack by the expected cost of an insider attack. An organization's risk exposure can then be used to determine the appropriate amount to spend on insider threat mitigation.

Recent research related to catastrophic events, or "low-probability, high-consequence occurrences" [Kleindorfer 2012], in the process industry [Kleindorfer 2007] and financial services industry [Muermann 2002] may provide strategies for insider threat mitigation. An organization can better understand the impact of an insider attack by understanding its warning signs. These warning signs often come in the form of a near miss: "an event, observation, or situation that possesses the potential for improving a system's safety and/or operability by reducing the risk of upsets, some of which may eventually cause serious damage" [Oktem 2003]. UITs can often be considered near misses in that they expose potential attack vectors and methods for exfiltration.

Consider the following incident. An employee at a Fortune 500 organization is working late into the night to finish her portion of the organization's quarterly forecast. She is working on the spreadsheet containing all of the organization's forecasts for production, shipping, and supplier pricing. Tired after a long day at work, the employee writes an email to her boss, attaches the spreadsheet, and goes to sleep. The next morning, the employee opens her email to find a response to her message: "Thanks for this data, it looks like you put a lot of effort into it."

The message was written by a writer for the largest trade magazine in the industry. The employee immediately reports the mistake to her boss, who notifies the legal office and executives of the mistake. The organization contacts the trade magazine and demands that the data be destroyed, and nothing is published. After the fact, the employee realizes that her email client had auto-completed the writer's address.

This actual incident, along with many of the UIT incidents analyzed for this report, represent the opportunity for the organization to analyze a near miss. By considering the near misses, organizations can better understand the probability of insider harm, the scale, and the consequences for the organization.

Oktem developed an eight-step process for addressing near misses in organizations [Oktem 2003]. The steps, adapted for an insider threat team, appear below:

1. Identification—Employees in the insider threat detection team must know the definition of a near miss and be trained to identify a near miss.
2. Disclosure (Reporting)—All near misses must be tracked by the organization. A database designed to record realized UITs and near misses may provide a valuable resource for understanding the potential impact of an incident.
3. Prioritization—Near-miss UIT cases must be ranked according to their potential impact to the organization.
4. Distribution—The highest impact near misses should be reported to those who have the potential to create a similar incident.
5. Identification of Causes (Causal Analysis)—The organization should determine the root cause or causes of the near-miss incidents and determine if the near miss reveals a vulnerability that could be exploited by malicious attackers. In the case of a phishing attack, the cause might be a lack of training and awareness.
6. Solution Identification—Once the root cause is understood, the organization should develop a solution or solutions to address the vulnerability. In the case of phishing, the solution may be to provide training to increase awareness.
7. Dissemination—In addition to the unintentional insider in the case, solutions should be communicated to those in the organization who were impacted or have the potential to be impacted by the near miss. In the case of a phishing attack, the organization might provide training to those with access to the organization's critical assets.
8. Resolution (Tracking)—An organization should track solutions as well as identify related, future near misses.

Oktem's work further describes the important aspects of a "Near-Miss Management System." Implementing such a system in the context of an information security team would enable a better understanding of the probability of a UIT incident as well as a better security posture.

5 Recommendations

The research results to this point are limited by the small sample size of available cases. As our collection of sample cases increases, we can better determine the validity of the initial findings of the research. To advance the current practice and state of the art in computer and network defense, especially safeguards against phishing and other social engineering attacks, organizations should prepare and test their ability to prevent, detect, and respond to the incidents covered in this report by following the best practices in the *Common Sense Guide to Mitigating Insider Threats, 4th Edition* [CERT 2012], as well as the mitigation strategies the Insider Threat Team outlined in the *UIT: Foundational Study* [CERT 2013].

To help the research community determine the level and means of prevention and mitigation for this kind of threat, the following research needs should be addressed across the cyber community:

- Develop an extensive, confidential, self-reporting UIT database. The database should track the security equivalent of near-miss incidents tracked by many healthcare and manufacturing organizations. A UIT database could be used to track the quality of security at an organization over time and to better assess the potential impact of a malicious insider attack.
- Perform more detailed analysis of UIT credentials and malware incidents and near incidents to inform the development of more effective mitigation approaches and tools.

5.1 Research Needs

We conclude that many of the research needs identified in the *UIT: Social Engineering* report [CERT 2014] are still valid and would be useful for addressing the UIT malware cases identified here. The earlier report's recommendations are summarized below.

5.1.1 Development of an Extensive UIT Database

A major roadblock to advancing our understanding of UIT social engineering exploits, such as PHISHING/SOCIAL incidents, and our ability to counter them is a dearth of data from actual incidents. By conducting public searches, we have collected a small number of cases that contain limited details, but we expect that far more case information could be obtained directly from affected organizations. In addition, a self-reporting mechanism is needed to collect and analyze incidents of social engineering. We recommend that a feasibility analysis be conducted to assess whether organizations could be motivated to self-report incidents, how the data may be collected anonymously and nonpunitively, and how the database can collect sensitive information from organizations across the spectrum of the economy [CERT 2014].

5.1.2 Detailed Analysis of UIT Incidents

Further research is needed to examine UIT incidents across a broad spectrum of participants in a comprehensive range of industries representing the full breadth of the economy. This research should focus on what factors are present in UIT incidents, how the affected organizations have handled these incidents, and the motivation of those conducting the PHISHING/SOCIAL or Malware exploits. Our current efforts were hampered by having access only to court transcripts and other third-party accounts of the incidents because organizations do not tend to make this information publicly available, even to research institutions. Only by collecting more detailed data and applying analysis and conceptual modeling approaches, such as those described in our previous report [CERT 2014], will we, as a community, be able to advance our understanding of UIT social engineering.

References/Bibliography

URLs are valid as of the publication date of this document.

[Beyer 1997]
Beyer, H. & Holtzblatt, K. *Contextual Design: Defining Customer-Centered Systems.* Elsevier, 1997.

[CERT 2013]
CERT Insider Threat Team. *Unintentional Insider Threats: A Foundational Study* (CMU/SEI-2013-TN-022). Software Engineering Institute, Carnegie Mellon University, 2013. http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=58744

[CERT 2014]
CERT Insider Threat Center. *Unintentional Insider Threats: Social Engineering* (CMU/SEI-2013-TN-024). Software Engineering Institute, Carnegie Mellon University, 2014. http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=77455

[Holtzblatt 2005]
Holtzblatt, K.; Wendell, J. B.; & Wood, S. *Rapid Contextual Design: A How-To Guide to Key Techniques for User-Centered Design.* Elsevier, 2005.

[Kleindorfer 2007]
Kleindorfer, P. R.; Lowe, R. A.; Rosenthal, I.; Rongwei, F.; & Belke, J. C. *Accident Epidemiology and the RMP Rule: Learning from a Decade of Accident History Data for the U.S. Chemical Industry* Final Report for Cooperative Agreement R-83033301). The Wharton School of the University of Pennsylvania, 2007.

[Kleindorfer 2012]
Kleindorfer, P.; Oktem, U. G.; Pariyani, A.; & Seider, W. D. “Assessment of Catastrophe Risk and Potential Losses in Industry.” *Computers & Chemical Engineering 47*, 20 (December 2012): 85-96.

[Muermann 2002]
Muermann, A. & Oktem, U. “The Near-Miss Management of Operational Risk.” *Journal of Risk Finance 4* (Fall 2002): 25-36.

[Oktem 2003]
U. G. Oktem. “Near-Miss: A Tool for Integrated Safety, Health, Environmental and Security Management.” *37th Annual AIChE Loss Prevention Symposium “Integration of Safety and Environmental Concepts.”* New Orleans, LA, March, 2003.

[Ponemon 2013]
Ponemon. *2013 Cost of Cyber Crime Study: United States.* Ponemon Institute, October 2013.

[SolarWinds 2014]
SolarWinds. *SolarWinds Federal Cybersecurity Survey Summary Report.* SolarWinds, 2014.

[Symantec 2014]
Symantec. “Internet Security Threat Report 2014.” *2013 Trends 19* (April 2014). Symantec Corporation.

[Verizon 2013]
Verizon. *2013 Data Breach Investigations Report.* Verizon, 2013.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. AGENCY USE ONLY (Leave Blank)	2. REPORT DATE July 2014	3. REPORT TYPE AND DATES COVERED Final
4. TITLE AND SUBTITLE Unintentional Insider Threats: A Review of Phishing and Malware Incidents by Economic Sector		5. FUNDING NUMBERS FA8721-05-C-0003
6. AUTHOR(S) CERT Insider Threat Team		
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213		8. PERFORMING ORGANIZATION REPORT NUMBER CMU/SEI-2014-TN-007
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) AFLCMC/PZE/Hanscom Enterprise Acquisition Division 20 Schilling Circle Building 1305 Hanscom AFB, MA 01731-2116		10. SPONSORING/MONITORING AGENCY REPORT NUMBER n/a
11. SUPPLEMENTARY NOTES		
12A DISTRIBUTION/AVAILABILITY STATEMENT Unclassified/Unlimited, DTIC, NTIS		12B DISTRIBUTION CODE

13. ABSTRACT (MAXIMUM 200 WORDS)

The research documented in this report seeks to advance the understanding of the unintentional insider threat (UIT) that results from phishing and other social engineering cases, specifically those involving malicious software (malware). The research team collected and analyzed publicly reported phishing cases involving malware and performed an initial analysis of the industry sectors impacted by this type of incident. This report provides that analysis as well as case examples and potential recommendations for mitigating UITs stemming from phishing and other social engineering incidents. The report also compares security offices' current practice of UIT monitoring to the current manufacturing and healthcare industries' practice of tracking near misses of adverse events.

14. SUBJECT TERMS unintentional insider threat, malware, social threat vector, cases, phishing	15. NUMBER OF PAGES 41
16. PRICE CODE	

17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UL