# On Social Engineering Attacks and Unintended Data Disclosures: Two Major Categories of End-User Cybersecurity Error

**John W. COFFEY**
**Department of Computer Science**
**The University of West Florida**
**Pensacola, FL. 32514, USA**
**jcoffey@uwf.edu**

**ABSTRACT**

End user error continues to be a significant root cause of cybersecurity data breaches. Despite widespread progress in the establishment of training for end users and a slight downward trend in end user error-mediated compromises as a percentage of total successful attacks and data breaches, the absolute number of successful attacks and the overall amount of disclosed data continue to trend upward. Reporting of data breaches remains problematic, as will be described here. Modern social engineering attacks are sophisticated occurrences that bear little resemblance to early, primitive phishing exploits, and despite large increases in end-user training, they still succeed. Significant amounts of sensitive data continue to be exposed by unintended data disclosures not precipitated by social engineering attacks. While organizations are awash in broad guidelines for the implementation of training programs, most guidelines do not provide details on the most common and most damaging types of breaches. A detailed analysis of the Privacy Rights Clearinghouse database of data breaches reveals patterns of errors that end users make that can inform the creation of more highly focused training programs.

## 1. INTRODUCTION

Cybersecurity research has a strong focus on technological solutions to vulnerabilities. However, human factors in cybersecurity breaches still loom large. Threats originate both from inside and outside organizations. Errors by end users and system administrators inside an organization create many opportunities for malicious actors who may also be inside or outside the organization. In order to address human error concerns, widespread training for end users has been put in place. Despite these pervasive efforts, the absolute number of end user error-mediated compromises continues to trend upward.

This article addresses details regarding two major categories of end user error: failure to detect social engineering attacks (and the consequences of such failures) and unintended data disclosures not resulting from social engineering attacks. It will briefly address the evolution of social engineering attacks, modern forms, and attributes of susceptible users, including the important role of social media in helping attackers create highly targeted attacks.

Significant amounts of sensitive data continue to be exposed by unintended data disclosures not precipitated by social engineering attacks. This work explores details regarding causes of unintended data disclosures, and problems with consistent and accurate reporting. The current work also identifies a vicious cycle of unintended data breaches providing sensitive personal information that can be used in highly targeted social engineering attacks. Successful social engineering attacks, particularly of the spear phishing variety, allow attackers access to sensitive information that can be used in further attacks. The use of social media plays an important role in helping attackers create highly targeted attacks that can start this cycle.

Although organizations have access to broad guidelines for the implementation of training programs and numerous prepackaged training courses, most guidelines do not provide details on the most common and most damaging causes of breaches. This work will provide a detailed analysis of a comprehensive database of unintended data disclosures citing the most commonly occurring precipitating events. Summarization of detailed data in service of more focused end-user training is one goal of this work.

The rest of this paper will provide insights into the overall picture of vulnerabilities caused by insiders vs outsiders, and modern social engineering attacks with a particular focus on spear phishing. A detailed analysis of the *Privacy Rights Clearinghouse* database of data breaches reveals patterns of errors that end users make that are discussed in service of more targeted training programs. The article closes with a consideration of the synergistic effects of successful spear phishing attacks and unintended data disclosures, and indications regarding how to break the vicious cycle these two problems entail.

## 2. UNINTENDED DATA DISCLOSURES

Unintended data disclosures remain a significant cybersecurity problem. They can occur as a result of deliberate or accidental actions by people inside an organization, as a result of deliberate actions by people outside a target organization, or through a combination of both inside and outside actors. The following sections contain descriptions of the insider vs outsider threat issue, a source for information regarding unintended data disclosures, and reasons why data breach reporting is inconsistent and essentially deficient.

### 2.1 Outsider vs Insider Threats

A multi-layered technological approach to cybersecurity is the best available means to ameliorate outsider attacks. While it is clear that outside attackers are more likely to act in a malicious way with a company's data, a consensus of experts suggests that the source of the greatest risk is from insiders [7]. Although insiders who mean no harm have access to large volumes of sensitive data that might be compromised, large percentages of them are unable to articulate any real understanding of IT-security related issues. Threats posed by insiders have led to the creation of a formal vocabulary to describe such threats in machine processable form [4].

Statistics pertaining to insider vs outsider attacks can hinge upon varying assumptions. Statistics pertaining to insider-mediated breaches often do not capture a significant fraction of instances of inside assist or insider negligent acts that facilitate an outside attack. Implications of the pervasive problem of insider threats (from both accidental and deliberate actions) include damaging, unintentional disclosure of sensitive data. This problem is discussed in the next section.

### 2.2 A Data Source for the Assessment of Unintended Data Disclosures

An organization named the Privacy Rights ClearingHouse (PRC) [6] has collected one of the most comprehensive records of data breaches in the United States since 2005, documenting more than 8000 breaches, large and small. The PRC was founded in 1992 at the Center for Public Interest Law at the University of San Diego School of Law. The PRC seeks to identify and bring attention to critical privacy-related issues.

For instance, the PRC was the first consumer organization in the nation to raise awareness of the concept of *identity theft* and to provide assistance to victims. PRC has worked for passage of several landmark laws including California law that addresses data breach notification requirements and security freeze law. In the wake of the Equifax breach, many people choose to protect themselves by freezing credit reports from the credit bureaus. PRC played a part in originating the law that afforded consumers this prerogative. PRC participates in state and federal public policy task forces pertaining to privacy legislation and administrative agency proceedings.

### 2.3 An Analyisis of the PRC Data on Unintended Disclosures

An analysis of the PRC data on unintended disclosures reveals that data breaches take a variety of forms. The database contains data on a total of 984 unintended data disclosure incidents between 2005 and 2017, in which some 215,000,000 records were disclosed. The most common form of unintended disclosure, occurring in 43% of documented cases, was through placement of sensitive data on websites or file sharing services. Often, the data were placed on secured systems that were later made public, or sensitive data were placed inadvertently on a publically accessible system along with data that legitimately belonged there.

Unintended disclosures through errors in email were the second most commonly occurring means of disclosure, accounting for 13% of cases documented by the PRC in that time period. Errors took the form of sending sensitive information to the wrong recipient, including sensitive data concerning other people in an email to a person who was properly receiving data about him or herself, and other, similar types of mistakes.

Unintended disclosures occurred in 13% of the cases through regular mail. A surprisingly large range of errors were made with regular mail from printing sensitive information such as social security numbers on mailing labels, to the inclusion of sensitive information pertaining to other people than the intended recipient in a mailing. After those top three causes, disclosures through unknown causes at 10% was fourth most common. Interestingly, of the 103 cases in which the cause of the disclosure was unknown, 89 occurred in healthcare. For more details regarding this analysis, please see [10].

These data point to specific root causes of the problem of unintended data disclosures and to the possibility of more targeted training for those who are responsible for the control and protection of sensitive data. At the

same time, the alarmingly large number of cases in which the cause of the unintended disclosure is unknown is problematic and must be addressed in itself. The following sections contain discussions of why available information pertaining to unintended data breaches remains incomplete, inconsistent, and generally problematic.

### 2.3 Difficulties in Data Breach reporting

Although the PRC goes to great lengths to accumulate and report findings of data breaches, the database has significant deficiencies. In many cases, the number of records breached is estimated; often the number is unknown. Of the 984 cases of unintentional disclosure, 279 cases (28%) involved an unknown number of records. As mentioned, a significant number of cases involving medical records reveal an unknown number of records and no particulars regarding how the breached occurred.

In some cases, the total number of records breached is reported but without details regarding the amount of unique sensitive information. Sometimes the narratives provide ranges such as "between 5,600 and 23,000 patients were affected." In some cases, a total is given as "estimated that more than half exposed social security numbers." Some of the narratives are vague regarding whether physical or electronic data was compromised.

### 2.4 Why breach reporting is Inconsistent.

The National Council of State Legislatures publishes state reporting guidelines for data breaches in the United States. Currently all 50 states, the District of Columbia, Guan, Puerto Rico and the Virgin Islands have (separate) reporting requirements. The states of Alabama and South Dakota only required data breach reporting in the last year. A typical reporting policy is long, technical, jargon-filled, and contains significant legalese.

Laws pertaining to reporting requirements typically specify:

- a taxonomy of organizations (such as the one utilized by the PRC, but often different) and potentially varying reporting requirements by organization type
- specific (but varying) definitions of what constitutes personal information
- the type of event that meets criteria as a breach and must be reported
- the type of notice that must be given
- exemptions from reporting, if any.

### 2.5 The Changing Nature of the Threat

Givens [1] states that wide adoption of EMV chip cards is expected to result in less credit and debit card fraud over time. A likely consequence of this improvement in payment card security that the focus of illegal activity going forward is expected to move to new account fraud, meaning that individuals' Social Security numbers will be in high demand.

Entities with large quantities of social security numbers and other personal information including governmental agencies, universities, and health care organizations are likely to be targeted. Healthcare institutions will continue to be targeted. The value of medical records is estimated to be up to 10 times that of credit and debit card data on the black market.

## 3. SOCIAL ENGINEERING ATTACKS

Social Engineering Attacks are attacks employed to trick, coerce or otherwise cause a person to perform an action the attacker wants done. Social engineering attacks have a long history on the Internet from primitive scattershot attempts to lure targets into providing up-front money in the hope of later gain, to modern, sophisticated, highly targeted attacks based upon in-depth knowledge of the targets of the attack. Social engineering attacks take a variety of forms as described in the next section.

### 3.1 Categories of Social Engineering Attacks

Social engineering attacks take on a variety of forms. The following list of categories of social engineering attacks is adapted from [2].

- **Phishing**: The attacker attempts to get the target to provide sensitive information such as login credentials or to access a website that will install malware on the target's machine.
- **Spear Phishing** (subset of Phishing) Attacks directed at specific individuals about whom a great deal is known, in which the attacker appears to be someone the target knows or should otherwise trust.
- **Baiting** Attackers leave removeable devices containing malware in public places with the hope that someone will pick them up out of curiosity and use them in their devices.
- **Tailgating** attackers exploit authorized persons to get access to restricted areas.
- **Quid pro quo** involves an exchange of something with the target in exchange for some benefit such as access or sharing of sensitive information.

Phishing attacks are of particular interest. They are so pervasive and successful that the Anti-phishing Working Group, a large-scale NGO, has been established to ameliorate damage done by phishing attacks [5]. Phishing is a type of social engineering attack often used to steal user data including login credentials, credit card numbers and other monetizable of weaponizable personal information. In a phishing attack, an attacker, masquerading as a trusted entity, typically tries to dupe a victim into opening an email, instant message, or text message.

The target is then tricked into clicking a link to a malicious website. Phishing is often used to gain a foothold in corporate or governmental networks as a part of a larger attack, such as an advanced persistent threat (APT) event. One possible scenario for a phishing attack: A spoofed email ostensibly from an actual university is mass-distributed to as many faculty members as possible. The email claims that the user's password is about to expire. Instructions are given to go to a page to renew their password within 24 hours. In such attacks, care is taken by the attackers to make the email look legitimate.

### 3.2 Spear Phishing

Spear phishing [9] is an email or electronic communications scam targeted towards a specific individual within an organization or business. Spear Phishing attacks typically are in service of stealing data for malicious purposes, or installing malware on a targeted user's computer.

In spear phishing attacks, an email arrives, apparently from a trustworthy source. The correspondence leads the unknowing recipient to a bogus website that contains malware the attacker wishes to install on the victim's machine. The emails use various tactics to get the victims' attention or to instill trust.

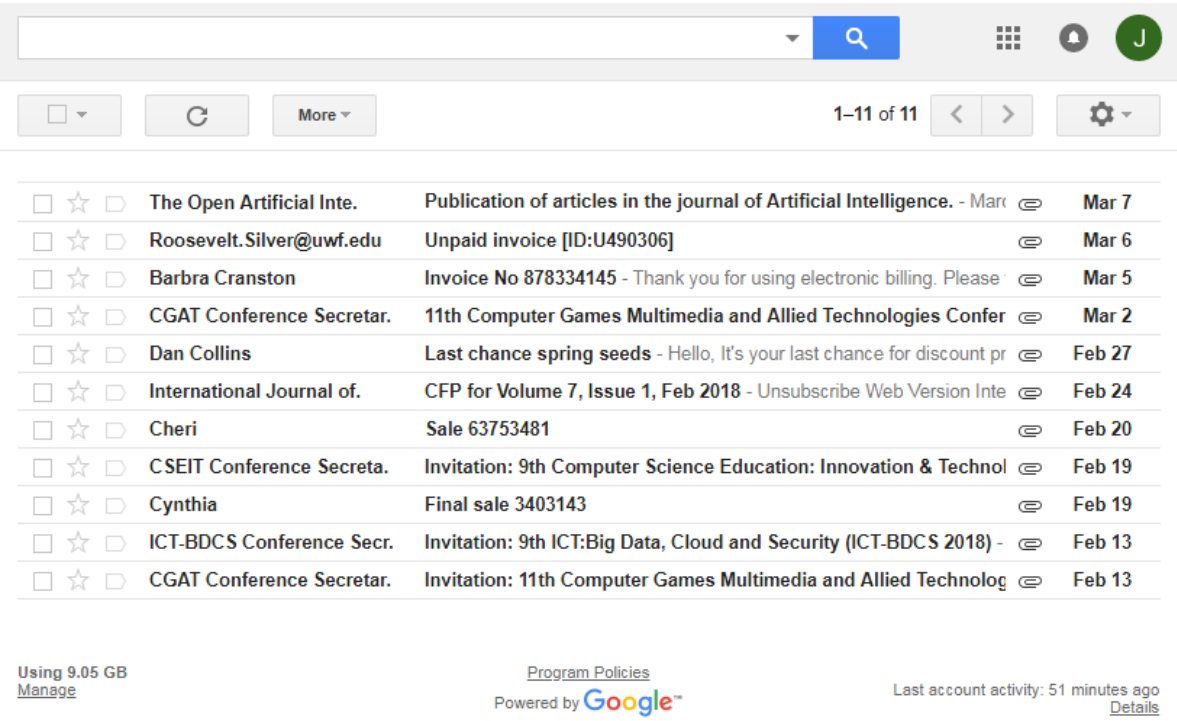


**Figure 1. An illustration of probable malware attachments from a one-month period.**

According to [9], more than 70% of spear phishing attacks were directed at 10 or fewer accounts. Approximately a third were directed at a single account. Spear phishing attacks tend to be of short duration and they are carefully arranged to avoid spam filters. Figure 1 contains a graphic of the author's collection of email that contained attachments from unknown outsiders over a one-month period. Of the eleven emails, seven were from conferences and likely (but not assuredly) legitimate, but four are clearly phishing attempts. The second entry, professing to be from the author's institution, is presenting an unpaid invoice. It is clearly bogus and dangerous. The third and seventh entries are again seeking to have the recipient pay a bill, potentially providing the attacker with credit card or bank details. Frequently,

government-sponsored hackers are behind these attacks. Cybercriminals do the same with the intention to resell confidential data to governments and private companies.

Mediation of the threat requires both technological safeguards and increased human awareness of this type of threat. Human Safeguards include ongoing vigilance to make employees aware of the evolving threat environments, from very basic threats to highly sophisticated, difficult to detect attacks. Ongoing training is not fool-proof but it is the best defense against those attacks that cannot be prevented by purely technological means. Training efforts by organizations tend to wax and wane over time.

Technological Safeguards include email protection solutions use anomalytics [8] to detect suspicious emails. Spam detectors are becoming more sophisticated. For example, the four obviously suspicious emails in Figure 1 were all placed in the spam folder. Additionally, dynamic malware analysis tools can analyze the destination websites for malicious behavior. Sandboxing at the time of delivery of a suspicious email or when users click on a URL is another defensive measure.

**www.campusclarity.com/tool-and-resources/administrative-tools/**
**www.campusclarity.com.tool-and-resources.com/administrative-tools/**
**www.campusclarify.com/tool-and-resources/administrative-tools/**

**Figure 2. A legitimate URL and two cousin domain URLs.**

### 3.3 Cousin Domains

Cousin Domains [3] are registered domain names used by criminals that are deceptively similar to legitimate domain names. The concept behind an attack based upon cousin domains is simple: the target name is familiar to many end-users, and therefore imparts a degree of trust. Often, essential parts of the legitimate name are embedded in the cousin domain name. Often the differences can be extremely subtle. For instance, the cousin domain might use some variant of the target name, such as replacing '1' with 'l' (e.g. 'company1.example' to attack 'companyl.example'). This latter form is sometimes known as a "homograph attack". For computer security people, the problems associated with cousin domains are difficult. Figure 2 contains three URLs, one of which is legitimate, and two, while highly similar, are not. Fostering sufficient vigilance to detect cousin domains in time-pressed computer users is a difficult problem.

## 4. SYNERGIES BETWEEN SPEAR PHISHING AND UNINTENDED DATA DISCLOSURES

A very specific form of synergy exists between unintended disclosures of sensitive personal information and spear phishing attacks. Spear phishing attacks rely on detailed information pertaining to individuals. Knowledge of an individual's health issues, particulars regarding a person's hobbies, job performance at work, or friends, and similar types of personal information can be used by attackers to gain trust. A fabricated trust relationship can be used to facilitate an unintended data disclosure. Sensitive personal information can be used as a weapon to increase the probability of success in further targeted phishing attacks. Figure 3 illustrates this vicious cycle.

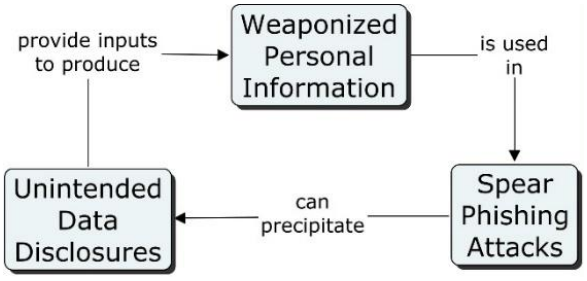


**Figure 3. The vicious cycle of unintended data disclosures and spear phishing attacks.**

## 5. SOLUTIONS TO THIS PROBLEM

The vicious cycle described in Figure 3 can be disrupted at any point. For instance, diminishing unintended disclosure of sensitive personal information that can be weaponized is helpful. With a smaller supply of detailed personal information, spear phishing attacks may become less frequent and less effective, in turn diminishing the amount of unintended data that is disclosed. Ideally, both targeted attacks and other causes of disclosures should be addressed simultaneously.

Both technological solutions and improved human factors are needed to break this cycle. Technological vulnerabilites are addressed by more secure software development and by improved systems administration. Improved Baccalaureate education and systems of certifications are needed to improve technical support for secure systems. End-user mediated vulnerabilites are addressed by more (and more frequent) and better training programs.

The fact that both technological solutions and human issues are involved would suggest that interdisciplinary work is needed to mediate these threats. Researchers studying end user error need to share knowledge of the types of errors users make with developers, systems administrators and technical educators/trainers. Developers can then focus on enhanced measures to protect users from themselves. Systems administrators can keep systems updated and can issue alerts to specific threats. Educators can create training materials that emphasize the particular threats that have been identified. Furthermore, researchers studying methods and practitioners who harden systems share information on limitations on their abilities to afford protections with educators. Knowledge of such limitations feeds into educational programs.

## 6. CONCLUSIONS

End user error is still responsible for highly damaging security breaches and unintended data disclosures. This work profiles the most commonly occurring types of unintended data disclosures. They vary by industry/government group. Reporting is highly variable and complicates adequately characterizing the problem. Phishing attacks have evolved significantly in sophistication over the years. There is a vicious cycle of unintended data disclosures providing personal information that can be used in phishing attacks that lead to more unintended disclosures. Both human and technological interventions are required to ameliorate these problems and information exchange can help better address them.

## 7. REFERENCES


[1] Givens, B. 2016. An On-the-Ground Look at Consumer Impacts of Data Breaches PRC. Online, Available at https://www.privacyrights.org/blog/ground-look-consumer-impacts-data-breaches

[2] Tiwari, A. 2017. What Is Social Engineering? What Are Different Types Of Social Engineering Attacks? Online, Available: https://fossbytes.com/what-is-social-engineering-types-techniques/

[3] Agari. 2015. Don't Let Your Customers Be Fooled By Cousin Domains. Online, Available at: https://www.agari.com/dont-let-your-customers-be-fooled-by-cousin-domains/

[4] Costa, D, Albrethsen, M., Collins, M., et al. 2016. An Insider Threat Indicator Ontology. https://resources.sei.cmu.edu/asset_files/TechnicalReport/2016_005_001_454627.pdf

[5] APWG. 2018. Unifying the Global Response to Cybercrime. Online, Available: https://antiphishing.org//

[6] Privacy Rights Clearinghouse. 2018. Empowering Consumers. Protecting Privacy. Online, Available: https://www.privacyrights.org/

[7] Giandomenico, N., and de Groot, J. 2016. Insider vs. Outsider Data Security Threats: What's the Greater Risk? Online. Available: https://digitalguardian.com/blog/insider-outsider-data-security-threats

[8] Hossein, E. (2015). Anomalytics & Cyber Security in the 21st Century. Online, Available: https://www.linkedin.com/pulse/anomalytics-cyber-security-21st-century-dr-hossein-eslambolchi

[9] Martinez, J. 2017. Spear-Phishing Attacks: What You Need to Know. Online, Available: https://www.pcmag.com/article/354240/spear-phishing-attacks-what-you-need-to-know.

[10] Coffey, J.W. 2017. An Analysis of Inadvertant Data Disclosure Incidents, 2005-2017. International Journal of Cyber-Security and Digital Forensics. 6(2). pp 84-91.