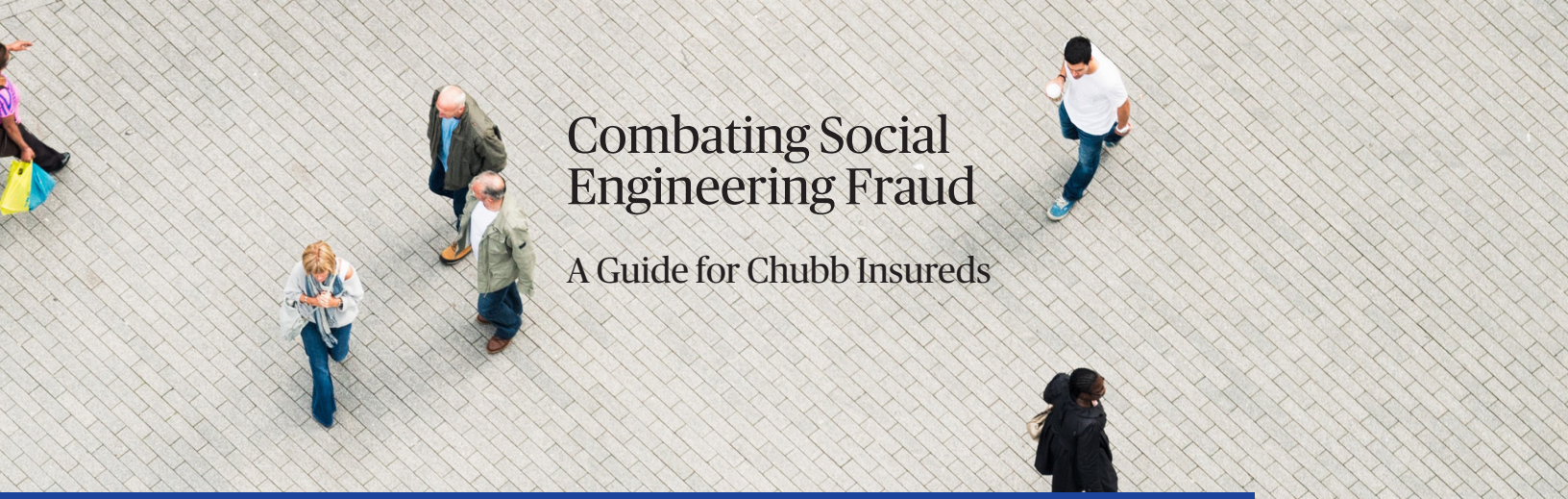


# Combating Social Engineering Fraud

## A Guide for Chubb Insureds

CHUBB®

Technology is advancing every second. While these advancements make our lives less cumbersome, they also come with new ways to infiltrate your business, despite having security measures in place. Fortunately, without requiring substantial capital investment, reevaluating how business is conducted in our fast-paced, modern world can reduce the likelihood of becoming a victim of the latest Social Engineering scam.

Social Engineering is the art of influencing people to disclose or give access to information that they would not typically provide; this method relies on human interaction rather than attempting to hack into a computer network. The criminals typically follow a four-step method:

- Gather information
- Develop a relationship
- Exploit trust
- Execute their scam

Social Engineering scams employ a wide range of methods and tactics to victimize people and businesses, including emailing malicious links, making phone calls, and following a person into a secure location. Recent scams include **phishing**, which involves someone claiming to be in a position of authority asking for confidential information, such as a password, or sending an email attachment that is infected with malware or spyware. The email may appear to come from a trusted employee, a supplier, or even a customer. It often requests banking and payment details be changed, or urgent payments be processed via wire transfer to new accounts. **Vishing and Smishing** is the practice of using fraudulent phone calls or text messages, respectively, to extract financial data from users for purposes of identity theft. **Piggybacking** is the term used when someone without proper credentials gains access to a restricted area, usually by physically following an employee.

Social Engineering scams are often successful because they exploit our natural tendency to trust each other and to believe information is credible rather than questionable. Further, in today's advanced technological environment, old processes that were sufficient in a "paper" world are now no longer effective at detecting and preventing fraud.

However, there are ways to protect yourself, your employees, and your business to mitigate the potential of falling prey to a Social Engineering scam. The most important preventative measures are a combination of strong policies and procedures, hardened IT security, and recurring employee education.

**Combating Social Engineering Fraud - A Guide for Chubb Insureds** provides you with a step-by-step, page-by-page evaluation process to assist you in determining where you may be vulnerable to potential Social Engineering schemes. This guide is intended for use by directors, facility managers, safety/risk managers, financial administrators, and independent security consultants. The guide includes suggestions for the implementation of security policies and procedures, operational controls, employee education, and technological controls.

This practical guide utilizes the following five key areas to assist in your evaluation of your current safeguards:

1. Electronic Security Policies
2. System Management Tools
3. Strength of Passwords
4. Compliance Testing (Phishing Campaigns)
5. Wire Transfer/ACH Policies

This guide and checklist is aimed at helping you and your team determine what level of protection should be considered minimal, or baseline, and provides further insight as to how you can optimize your protection. The guide also serves as a future record for your decision-making criteria and will help guide your decisions as you enhance your control framework.

## How to Use This Guide:

**Combating Social Engineering Fraud – A Guide for Chubb Insureds** enables you to evaluate your company using the same criteria for all locations. Here's a plan to get you and your team started:

1. Each section of this guide is important to the health of your company. Answer each question honestly.
2. Mark each question with Yes or No.
3. Score your answers to determine how prepared you are to resist a Social Engineering attack.

Use the Resources and Information pages to track your results and tally your answers.

## 1. Electronic Security Policy

In this section, consider the commingling of business and personal devices and their related accounts. Business and personal accounts and devices should have a clearly defined distinction in the workplace.

| Category | Yes | No | Comments |
|---|---|---|---|
| We have a documented Cyber Security policy. | | | |
| Employees understand the Cyber Security policy, as well as the importance of adhering to it. | | | |
| The Cyber Security Policy is adhered to on all company issued devices. | | | |
| We have a documented Bring Your Own Device policy. | | | |
| Employees understand the Bring Your Own Device policy, as well as the importance of adhering to it. | | | |

## 2. System Management Tools

In this section, review your access controls (both physical and online), system updates, and system testing to ensure all are properly managed and kept up-to-date.

| Category | Yes | No | Comments |
|---|---|---|---|
| Building entrances are equipped with access controls, such as a badge swipe. | | | |
| We have a documented policy regarding the security of building entrances, i.e. not propping doors open or allowing entrance to non-employees. | | | |
| Visitors/vendors are signed in upon entrance and recorded in a log. | | | |
| Visitors/vendors are escorted while in company buildings and/or facilities not designated for public use. | | | |
| Employees do not have more network access than is necessary to fulfill their job function. | | | |
| Computers are kept updated and patched at regular intervals, such as weekly. | | | |
| Employees do not have the ability to override or postpone updates/patches. | | | |
| Multi-Factor authentication has been activated on all business email accounts, particularly those accessed via a browser or outside of the company's firewall. | | | |

### 2. System Management Tools – continued

| Category | Yes | No | Comments |
|---|---|---|---|
| Spam-filters have been activated on business email accounts. | | | |
| External emails are identified as such upon arrival. (This is typically a free option provided by the domain host and can be set-up by the user.) | | | |
| An external security software program is utilized to assess incoming emails for threats (e.g., spam, imposter, phishing, etc.). | | | |
| The IT department has placed restrictions on internet usage and/or prohibited domains. | | | |
| Social media outlets are monitored for correct usage by employees and third parties. | | | |
| Unused/unnecessary network services and dormant URLs have been removed or deactivated. | | | |
| VPN or similar encryption has been added by IT to reach various points of the network. | | | |
| Data backup is performed weekly. | | | |
| Backed-up data is preserved and covers an adequate history. | | | |
| System firewall testing is performed regularly and documented. | | | |
| All compressed files are scanned for viruses before and after decompression. | | | |

### 3. Strength of Passwords

In this section, you can evaluate your credentialing protocols. A strong password is one that is difficult for a machine to guess, but easy for a user to remember.

| Category | Yes | No | Comments |
|---|---|---|---|
| Passwords are required to contain at least 8-12 alpha-numeric characters, as well as special symbols. | | | |
| Multi-Factor Authentication has been activated on all accounts where it is offered by the program/software. | | | |
| Passwords are kept confidential and not shared with others. | | | |
| Passwords are prohibited to be recycled within a 90 day period. | | | |

### 4. Compliance Testing/Phishing Campaign

In this section, consider the breadth and depth to which your company makes training employees a priority. Employees need to feel a sense of ownership when it comes to security.

| Category | Yes | No | Comments |
|---|---|---|---|
| Annual Social Engineering training is conducted. | | | |
| Social Engineering is included as part of monthly refresher training topics. | | | |
| Internal phishing campaigns have been performed to track employee adherence to policy. | | | |
| Results of all internal phishing campaigns are shared with employees. | | | |
| Results of internal phishing campaigns are followed-up with refresher training for any employees who may need it. | | | |
| Employees are aware of what company information is considered confidential. | | | |
| Employees recognize and feel a part of security initiatives. | | | |
| New hires receive initial training regarding Social Engineering and cyber security, which is documented and kept in their employee file. | | | |
| Cyber security is stressed at all levels of the business, from the CEO or Owner downward. | | | |
| All employees receive training to scrutinize emails before opening any links or downloading any attachments. | | | |
| Personal email accounts are prohibited from being established on or accessed via company computers. | | | |

## 5. Wire Transfer/ACH Policies

In this section, evaluate the policies and procedures surrounding payment requests. Clear-cut policies and procedures should be in place and communicated with all employees who initiate or send wire transfers or ACH payments.

| Category | Yes | No | Comments |
|---|---|---|---|
| We have a documented Policy & Procedures manual for wire transfers/ACH payments. | | | |
| We have a documented policy regarding verification of payment requests from non-employees. | | | |
| We have a documented policy regarding verification of payment requests from internal parties, regardless of business ranking. | | | |
| Policies and procedures are reviewed with appropriate personnel as part of monthly refresher training. | | | |
| We have an authority matrix for dollar amounts of wire transfers/ACH payments that requires more employee involvement and seniority as the dollar value increases. For example:<br>• Up to $5,000 can be authorized by one employee<br>• $5,000 - $20,000, initiated by Employee X and authorized by Employee Y<br>• $20,000 - $50,000 initiated by Employee X, co-authorized by Employee Y and Employee Z | | | |
| We have policies and procedures in place to verify the accuracy of vendor or customer payment requests with a representative of the vendor or customer directly, independent of email. | | | |
| We have policies in place to verify the initiation and authorization of wire transfers/ACH payments verbally with the requester of the payment. | | | |
| Banking partners have agreed to verbally verify with you all funds transfer requests over a specified dollar amount. | | | |
| Online banking platforms have been configured to require that the same person cannot both initiate and authorize a wire transfer/ACH payment. | | | |
| Online banking platforms have been configured to limit the number and dollar value allowed during a preset period of time. | | | |
| We have policies and procedures in place to verify “emergency” or “urgent” requests for wire transfer/ACH payments. | | | |

## Company Evaluation

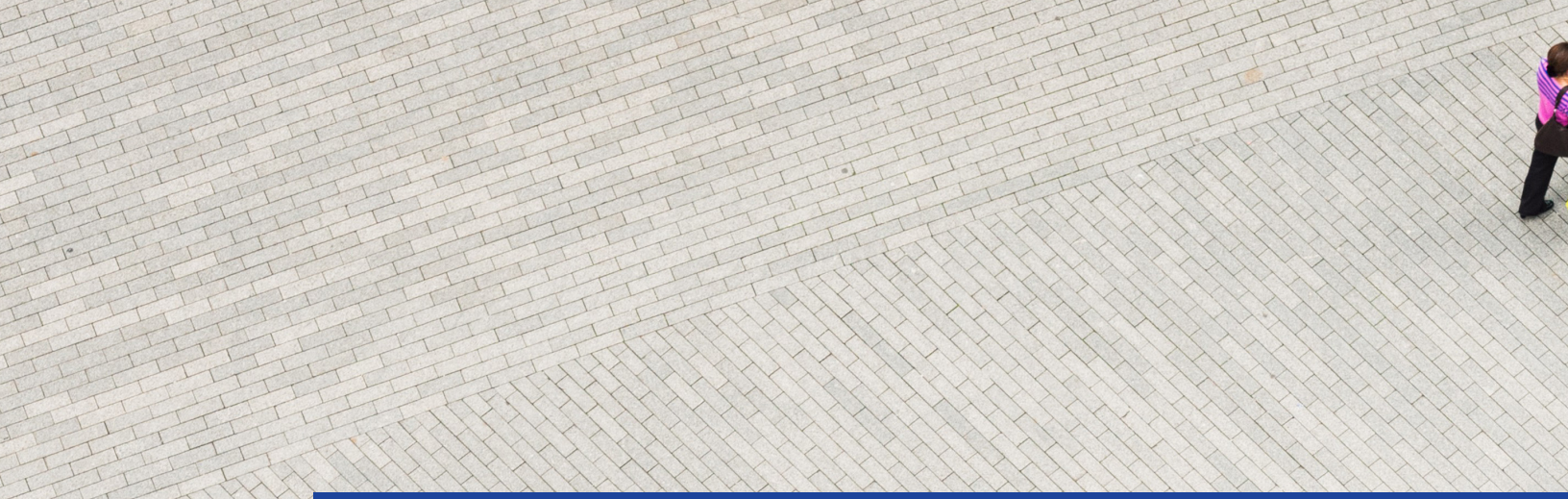
**How to Score Each Section:**
Review the guide and insert the total points for each category below (Yes = 2 points; No = 0 points.) As a result, the higher your score, the better prepared you are to resist a Social Engineering attack.

| Category | Total Points Possible | Your Score | Comments |
|---|---|---|---|
| 1. Electronic Security Policy | 10 | | |
| 2. System Management Tools | 38 | | |
| 3. Strength of Passwords | 8 | | |
| 4. Compliance Testing/Phishing Campaigns | 22 | | |
| 5. Wire Transfer/ACH Policies | 22 | | |
| **Total Score** | **100** | | |

There is no 100%, foolproof way to prevent social engineering and the frauds perpetrated by criminals adept at using these tactics. However, there are ways to protect against it, many of which do not require much more than a willingness to revisit and reevaluate processes to fit our modern world. Maintaining strong policies and procedures, consistent and persistent training and awareness, and vigilant system maintenance are all vital aspects of a good defense. Although the ultimate outcome of the criminal using social engineering tactics is to gain access to confidential information, invoices, wire transfer requests, and bank accounts, their attack always begins with your employees. A strong policy and appropriate procedures aren't effective if they are not consistently implemented and reinforced; one click, one divulged password, one employee wanting to be helpful can undermine all of your efforts.

If you scored low, or would like more information on protecting yourself and your business against Social Engineering attacks, please contact Lowers & Associates at (540) 338-7151 for a free consultation.

For more information about Chubb's Crime insurance products and services, contact Chris Arehart at carehart@chubb.com or visit www.chubb.com/us/crime.



# Chubb. Insured.[SM]