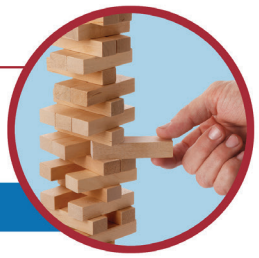
Utica National Insurance Group®

ERRORS & OMISSIONS

RISK MANAGEMENT ALERT



Social Engineering Risk Mitigation for Cyber Loss Exposures

As the member companies of the Utica National Insurance Group introduce three new coverages as part of our Cybersurance offering, we would like to suggest some pre-loss, risk management ideas to help prevent unauthorized intrusions into your agency systems. The security solutions you may have implemented may be rendered ineffective if your staff is unintentionally allowing access to your systems and information.

You may be unfamiliar with the concepts of Social Engineering and creating a Human Firewall in the context of information security. Social Engineering is defined as the use of deception to manipulate individuals into performing actions or divulging confidential or personal information that may be used for fraudulent purposes. A Human Firewall refers to the awareness level that all users must have to ensure that they themselves provide an effective layer of security.

Employee behavior can have a big impact on information security for organizations. If those with legitimate access to your network can be manipulated into revealing their passwords or allowing unauthorized people to use their computers, all of your information security tools may be worthless.

Many social engineers do not even possess a high level of technical skill. It is their "people skills" -- charm, trickery, or intimidation – that get them where they are not supposed to be by convincing legitimate employees to disclose information that compromises the security of data, computer systems, and networks.

So what can your agency do to reduce the likelihood of being the victim of Social Engineering fraud?

- The Human Firewall's best weapon is common sense.
- Provide Security Awareness training to ensure all staff is aware of potential threats and can recognize Social Engineering attempts.
- Use strong passwords or passphrases and implement multifactor authentication (MFA) wherever possible.
- Properly dispose of non-public information by shredding and do not leave non-public information unattended.
- Develop an incident response plan and test it periodically to ensure everyone knows how to respond to incidents and report them immediately to minimize any potential damage.
- Ensure you have a comprehensive set of information security policies and methods to ensure that everyone is consistently following them.

What are some key elements to include in security policies to mitigate Social Engineering risks?

- Possess strong password policies. (i.e. no generic accounts, all activity must be able to be traced to an individual, no sharing of accounts, penalties for violations, etc.)
- Data classification should clearly outline what information is considered non-public (i.e. personally identifiable information, private information, protected health information, etc).
- Build in device and software controls to regulate what users can and cannot do or install on their equipment and restrictions that they are used for work purposes only. Do not mix business with pleasure.
- Install anti-malware to ensure that a comprehensive solution is implemented to detect and block any malicious activity.
- Implement access controls for periodic (at least bi-annually) review of access to all systems. Keep evidence of the review and approval of the current access list by a senior manager.
- Monitor the actions of employees to validate that tasks performed are for work purposes and to detect abnormal activity.
- Employ data loss prevention tools to detect exfiltration of non-public information from your systems.
- Focus on physical security to ensure only authorized personnel have access to areas containing non-public information. Require that computers be locked by the user when they are left unattended. Do not rely on systematic locking mechanisms.
- Execute a risk assessment at least annually to evaluate the effectiveness of security controls and to understand any gaps.
- Perform a cybersecurity-focused risk assessment for all third-party service providers at least annually to ensure they also have implemented effective information security procedures.

Continued

What are some specifics employees should think about or ask themselves in order to prevent a possible Social Engineering incident?

- STOP and think!
- Did you request this information?
- Are you expecting this request?
- Do you know the person requesting this information or asking you to act?
- Are you the right person to provide this information?
- Is there a specific business reason you would be asked for this information?
- Are you being asked for personal information?
- Be very suspicious of "urgent" requests or those that rely on your goodwill and genuine desire to be helpful to others.
- Do NOT be curious. Don't open an attachment because it looks enticing or promises a benefit to you. Just delete it.
- Never divulge personal information via phone or unsecured websites.
- Do not click on links, download files, or open attachments from unknown senders.
- Be particularly aware of phone vishing as this tactic is becoming more popular
- Beware of pop-ups and never enter personal information in one.
- If it sounds too good to be true, it probably is.
- Nothing is free in the cyber world. If you sign up for a free coupon, free newsletter, social media site, realize that all of your information is being used and sold in the cyber world in some way or another.

Your most important asset is your people. That is also true when it comes to cybersecurity in your agency. **Educate them. Train them. Remind them to use their common sense. If it sounds "phishy," it probably is.**

Social Engineering Terms to Know:

- **Phishing** is an email, instant message (IM), comment, or text message that appears to come from a legitimate company, bank, school, or other institution, typically sent to several users.
- **Spear Phishing** is a phishing attempt that is targeted to a specific user or group.
- **Vishing or "Voice phishing"** uses the phone (cell or landline) to attempt to gather personal or financial information from the target.
- **Smishing** sends a text message to a cell phone to get the user to click on a link or reply by texting a random phone number or truncated number (i.e.: 44567)
- **Pretexting** is when an attacker pretends to legitimately need personal or financial data in order to confirm the identity of the recipient.
- **Baiting** is a popup or download request meant to get your attention to trick you into clicking on it. Some examples may be a free popular movie, song, item to purchase, free item, or monetary incentive. The victim is prompted to log in which typically grants remote access to the hacker or opens up access to your computer that the hacker will use later.
- **Scareware** involves tricking the victim into thinking the computer is infected with malware or they have inadvertently downloaded illegal or malicious content. The attacker offers to help the victim "fix" their computer by granting access to it.
- **Rogue** is malware that poses as security software to trick the victim into paying for the fake removal of malware.
- **Water holing** is when an attacker attempts to compromise a specific group of people by infecting websites the group is known to visit in order to gain network access.
- **Diversion theft** is when attackers try to trick a delivery company into going to the wrong location and try to intercept the delivery.
- **Tailgating** is when someone attempts to slip in behind a user with a valid building or secure area entry badge without having to swipe a badge.
- **Quid pro quo** is when an attacker pretends to provide something in exchange for the target information or assistance. A hacker may call a selection of random numbers within an organization and pretend to be calling back from a legitimate tech support group.
- **Honey trap** is when an attacker pretends to be a desirable person to interact with online or a person trying to establish a fake online relationship intended to gather sensitive information through that relationship.

Utica National Insurance Group
Insurance that starts with you.®
Utica Mutual Insurance Company and its affiliated companies, New Hartford, NY 13413
www.uticanational.com • 1.800.598.8422