Utica National's Errors & Omissions

RISK MANAGEMENT ALERT

We KNOW E&O for Insurance Agents

SOCIAL ENGINEERING RISK MITIGATION
Help Protect Your Agency from Cyber Loss Exposures

Your staff's behavior can have a big impact on your agency's information security. Your information security tools may be worthless if those with legitimate access to your network can be manipulated by "social engineers" into revealing their passwords or allowing unauthorized people to use their computers.

Social Engineering is the use of deception to manipulate individuals into performing actions or divulging confidential or personal information that may be used for fraudulent purposes. Many social engineers do not even possess a high level of technical skill. It's their "people skills" — charm, trickery, or intimidation – that get them where they are not supposed to be.

A Human Firewall is the awareness level that all users – your staff – must have to ensure that they provide an effective layer of security.

WAYS TO HELP REDUCE THE LIKELIHOOD OF BEING A VICTIM OF SOCIAL ENGINEERING FRAUD

1. **Provide security awareness training** to ensure all staff is aware of potential threats and can recognize Social Engineering attempts. The Human Firewall's best weapon is common sense.
2. **Use strong passwords or passphrases** and implement multifactor authentication (MFA) wherever possible.
3. **Properly dispose of non-public information by shredding** and do not leave non-public information unattended.
4. **Develop an incident response plan** and test it periodically to ensure everyone knows how to respond to incidents – including reporting them immediately to minimize any potential damage.
5. **Have a comprehensive set of information security policies and methods** to ensure everyone consistently follows them.

KEY ELEMENTS TO INCLUDE IN SECURITY POLICIES TO MITIGATE SOCIAL ENGINEERING RISKS

1. **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.).
2. **Clearly outline what information is considered non-public** (i.e., personally identifiable information, private information, protected health information, etc.).
3. **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.
4. **Install anti-malware** to ensure a comprehensive solution is implemented to detect and block malicious activity.

Continues

KEY ELEMENTS TO INCLUDE IN SECURITY POLICIES TO MITIGATE SOCIAL ENGINEERING RISKS (Cont.)

5. **Implement access controls for periodic review** (at least bi-annually) of access to all systems. Keep evidence of the review and approval of the current access list by a senior manager.

6. **Monitor employees' actions** to validate that tasks performed are for work purposes and to detect abnormal activity.

7. **Use data-loss prevention tools** to detect exfiltration of non-public information from your systems.

8. **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.

9. **Execute a risk assessment** at least annually to evaluate the effectiveness of security controls and to understand any gaps.

10. **Perform a cybersecurity-focused risk assessment for all third-party service providers** at least annually to ensure they also have effective information security procedures.

STOP AND THINK:

THINGS TO CONSIDER TO HELP PREVENT A SOCIAL ENGINEERING INCIDENT

- **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?
- **Never divulge personal information** by phone or unsecured websites.
- **Do not click on links, download files, or open attachments** from unknown senders.
- **Be 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 coupon, newsletter, or social media site, all of your information is used and sold in some way.
- **Be 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. *Delete it.*

YOUR PEOPLE
are your most important asset when it comes to your agency's cybersecurity.

Educate them.

Train them.

Remind them to use their common sense.

If it sounds "phishy," it probably is.

Continues

SOCIAL ENGINEERING TERMS TO KNOW

- **Phishing –** 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 –** a phishing attempt 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 –** a text message is sent to a cell phone to get the user to click a link or reply by texting a random phone number or truncated number (i.e.: 44567).
- **Pretexting –** an attacker pretends to legitimately need personal or financial data to confirm the recipient's identity.
- **Baiting –** a pop-up or download request meant to get your attention to trick you into clicking it. Examples include a free popular movie, song, or item, an item to purchase, 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 –** 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 –** malware that poses as security software to trick the victim into paying for the fake removal of malware.
- **Water holing –** an attacker attempts to compromise a specific group of people to gain network access by infecting websites the group is known to visit.
- **Diversion theft –** attackers try to trick a delivery company into going to the wrong location and try to intercept the delivery.
- **Tailgating –** 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 –** 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 –** 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.

5-R-1286 Ed. 02-2023 Utica National Insurance Group | *Utica Mutual Insurance Company and its affiliated companies New Hartford, NY 13413*