FORTRA™

GUIDE (TERRANOVA SECURITY)

How to Protect Your Data From Social Engineering

TABLE OF CONTENTS

What is Social Engineering?

Social engineering is a manipulation technique used by cybercriminals to deceive people into taking an action that would benefit the criminal. These cybercriminals are con artists that use technology to trick their victims.

Any successful cyber attack that employs social engineering preys on one basic human instinct: trust. Once that connection is established, a scammer can steal sensitive data and use it to commit additional crimes in the future.

For example, let's say a cybercriminal wants to convince an employee to divulge passwords that protect confidential organizational data. They can use social engineering tactics to disguise their true intent as a message coming from the help desk, a service provider, or a system requesting account validation.

In other cases, victims of social engineering attacks may think they're helping someone they know with an urgent matter. In reality, they're exposing themselves to security breaches that can lead to data leakage or malware installations on company devices or networks.

All it takes is one email, phone call, or text message that appears to be coming from a recognized person or organization to fall through the cracks. After the deception works and the attack succeeds, the cybercriminals can expose sensitive information, use it to their benefit, or take control of devices, systems and networks.

According to 2020 data, one-third of all breaches featured some form of phishing or social engineering. The latter can be difficult to safeguard against because, technology cannot stop 100% of the attacks and by their nature, human beings are unpredictable. To avoid these kinds of traps, all members of an organization must remain vigilant.

Why Social Engineering is So Effective

In short, social engineering is dangerous because people make mistakes.

Even though victims know they must be suspicious of emails that, for example, promise them refunds, or phone calls that tell them they'll be arrested if they don't disclose sensitive information, people still get caught off-guard.

Successful social engineering scams rely on that knee-jerk human reaction to trust the sender and believe the message, one that often supersedes established cyber security awareness habits. Being busy, not paying close enough attention, complacency, or simply forgetting cyber security basics – all these lapses can lead to users being too trustful.

For those reasons, it's not unheard of for people to become repeat victims of social engineering attacks. This is because changing individual human behavior, especially when it comes to reversing bad habits, involves more than simply having an idea of what to look for.

Because it preys on weaknesses brought about by human reflex, it's much easier for cybercriminals to use social engineering to hack a human than it is to hack an organization's systems or network.

By prioritizing a people-first approach to cyber security, you can provide all users the tools they need to steer clear of any social engineering attempts and consistently keep their data safe.

As a result...

Data breaches have only grown more significant in recent years. Cyber attacks exposed more than four billion user records during the first half of 2019 alone. Throw repeat clickers and ineffective security awareness training into that mix and an organization's risk factor increases substantially.

How Social Engineering Attacks Prey on Human Emotion

The best examples of social engineering are the ones that play all the right notes on a victim's emotional scale. If the user is not properly trained to recognize the patterns of common social engineering attacks, they can be hard to recognize.

Some sample emotions that cybercriminals exploit to execute a social engineering scheme include:

Fear

In most cases, fear manipulation involves a threat of severe consequences if the victim does not act quickly. This may come in the form of a voicemail claiming you are under investigation for tax fraud and ordering you to call immediately to prevent further criminal investigation. This is a very powerful lure, especially during tax season when stress about finances is high.

Greed

Imagine if you could transfer $10 to an investor and see it grow into $10,000, all without any effort on your end? Cybercriminals play both trust and greed off each other to convince victims that they can get something for nothing. A carefully worded email can bait victims into providing bank account information with the promise that funds will be transferred to them later that day.

Curiosity

Events receiving a lot of news coverage can be used to take advantage of human curiosity and trick victims into acting. For example, after the second Boeing MAX8 plane crash, when cybercriminals sent emails with attachments that supposedly contained leaked data about the incident. When clicked, the attachment installed a harmful software on the victim's computer.

Helpfulness

Cybercriminals may research an organization and target a handful of its employees with an email that appears to come from their manager(s). The email asks each victim to send their "manager" password data for administrative or accounting purposes, stressing that the information is needed to ensure everyone gets paid on time. The urgent tone triggers our innate impulse to be helpful.

Safety

Ironically enough, many social engineering attacks are centered around a request to protect sensitive user data. This can come in the form of a customer support email from a trusted online retailer, asking for credit card information to secure your account. By leveraging a company's branding elements and even parts of their website, cybercriminals make those messages seem even more real.

How to Spot Common Social Engineering Tactics

At the end of the day, the human element of cyber security is only as strong as its ability to detect and avoid incoming threats.

Every person within an organization, from front-line employees to managers and executives, must know what social engineering attacks look and/or sound like. Otherwise, the risk of data or system exposure through a malicious email link or attachment can increase significantly.

Let us take a closer look at the various forms that cybercriminals can use to package their social engineering attempts.

Baiting

Baiting is both an online and physical social engineering attack that promises the victim something in exchange for an action. This can include plugging in a USB key or downloading an attachment to receive free movie downloads for life. The computer and the network can be targets of malicious software that captures login credentials or sends fake email messages.

Malware Removal

The promise of malware removal messages tricks victims into paying for a tool to remove viruses or other nefarious software from their devices. Depending on the scam, the criminal can steal the victim's credit card information or install a different malware or ransomware program onto the computer or mobile device. Keep an eye out for malware emails – nearly 95% of payloads are delivered this way.

Phishing

Phishing encompasses a wide range of devious tactics, including deceptive emails, fake websites, and misleading text messages. They all have the same goal: to steal confidential data belonging to an individual or organization. Phishing attacks are typically successful when they appear to come from a trusted acquaintance or organizational entity.

Pretexting

Pretexting is a social engineering technique where a false identity dupes a victim into giving up sensitive information. For instance, a cybercriminal may know that the targeted individual recently bought an item from Apple and pretends to be a company customer service representative to acquire credit card information or other confidential details.

Quid Pro Quo

Quid pro quo scams rely on an exchange of information to convince a victim to act. Often, they offer to provide a service in exchange for a benefit. A common tactic in this category is when a cybercriminal impersonates an IT support employee and calls victims who recently opened a support ticket, promising to fix a virus-related issue if they are provided with login credentials.

Spear Phishing

Spear phishing is a cybercrime that deploys targeted attacks against individuals and businesses using relevant and well-crafted messages. Hackers will collect details about the targeted parties and, using email, use that information to appear familiar to the victim(s). Though often used simply to steal user data, spear phishing can also be a means to install malware or ransomware onto someone's device.

Tailgating

Tailgating is a physical social engineering technique, that relies on human trust, to gain access to a building or secure location therein. The criminal may simply walk closely behind someone and slip through an open door or ask to be buzzed in because they forgot their key card. This technique underscores the need for employees to pay attention to who is loitering near doors and never hesitate to ask for identification.

Vishing

Vishing uses phone calls or voicemail to convince victims that they need to act quickly. Typically, messages will dangle the threat of being subjected to legal action or a criminal attack, such as one urging the victim to reset their banking information because their account has been hacked.

Water-holing

Water-holing targets a group of users and websites they frequent. The cybercriminal looks for a security vulnerability in one of these websites and then infects it with malware. Eventually, a member of the targeted group will be victimized by the malware. This specific social engineering technique is also very hard to detect.

How to Protect Your Data from Social Engineering Attacks in 7 Steps

Simply telling users about social engineering in a one-off seminar or requiring them to watch a handful of educational videos on the topic will not fully protect your organization's data.

Instead, put employees in a position to succeed by building, maintaining, and optimizing a security awareness training infrastructure. This will keep everyone up to date on the latest threats and help them retain the right information and skills to ensure consistent cyber safety.

Here are some key areas to address:

1. **Invest in Behavior Change**
   To effectively reduce human risk, emphasize security awareness training that promotes behavior change. Take advantage of tools such as phishing simulations, ransomware simulations, and cyber security assessments to strengthen your organization.
2. **Educate your Employees with Effective Content**
   Arguably the most important factor in any security awareness initiative is high-quality educational content. Use assets like online courses, micro- and nanolearning modules, and nanovideo content to educate your team on social engineering scams. Also, use real-world examples to demonstrate how easy it is for anyone to be caught off-guard by related tactics.
3. **Expose Users to Practical Phishing Simulations**
   Educational content is important, but it is greatly enhanced when combined with practical simulations that test user knowledge in a safe environment. Use phishing simulations and other staged attacks to deepen everyone's learning experience and further promote positive behavior change.
4. **Make Sure Everyone Has Up-To-Date Information**
   Content and simulations must also be continually updated and redeployed to ensure that everyone is aware of current cyber threats in circulation. Providing employees with this information means there is a greater chance they will be able to identify and avoid a social engineering attempt.
5. **Create and Nurture a Security-First Culture**
   An underrated aspect of the data protection process has to do with an organization's security culture. Starting at the very top, creating and fostering environmental support for behavior change must be a major priority. This will inspire learning and support unilateral security awareness. Encourage users to reports suspicious activity, even after they have fallen victims to an attack.
6. **Encourage and Reward Organizational Ambassadors**
   Throughout the security awareness training process, it is crucial to appoint and reward internal program ambassadors to keep interest levels high. Create a group of internal cyber security heroes who are committed to keeping your organization cyber secure to encourage universal employee buy-in.
7. **Provide Ongoing Support with Engaging Campaigns**
   Provide ongoing communication and campaigns about social engineering, cyber security, and phishing with engaging communication tools. These will help ignite conversations and awareness about the risks that can come with suspicious emails, URLs, attachments, phone calls, and other forms of social engineering attacks.

Additional Resources

Blog Posts

- 9 Examples of Social Engineering Attacks
- What the Twitter Hack Revealed About Social Engineering
- 19 Examples of Common Phishing Emails

Free eBooks

- Improve Your Organization's Phishing Defenses and Strategies
- The Human Fix to Human Risk

Cyberpedia Page

- Social Engineering
- Phishing

Resources

- Top cybersecurity facts, figures and statistics for 2020 (CSO Online)
- 2020 Data Breach Investigations Report (Verizon)
- 2019 Data Breach QuickView Report (RiskBased Security)

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.