SOCIAL ENGINEERING: A CHEAT SHEET FOR BUSINESS PROFESSIONALS

TechRepublic

TABLE OF CONTENTS

SOCIAL ENGINEERING: A CHEAT SHEET FOR BUSINESS PROFESSIONALS

People, like computers, can be hacked using a process called social engineering, and there's a good chance a cybersecurity attack on your organization could start with this technique.

BY BRANDON VIGLIAROLO

We don't operate like computers--they only do what they're told, executing tasks based on a set of instructions, without the ability to critically assess the honesty or good faith of the person giving the input. At least, that's what we think is different about us and machines.

But that isn't the case at all: We humans, for all our smarts and ability to make critical judgements, are also prone to taking our instructions at face value without considering the honesty of the person asking us to do something. Hackers have learned this and turned it into a process called social engineering.

This human-hacking tactic is nothing new: Con artists have been performing social engineering tricks for centuries. In the age of cybercrimes and online scams, social engineering has become far more threatening: Con artists can now reach out and trick you without ever having to speak a word, and it's becoming one of the preferred methods of gaining illicit access to secure systems.

WHAT IS SOCIAL ENGINEERING?

Security consulting firm Social Engineer, Inc., defines social engineering in incredibly basic and broadterms: "Any act that influences a person to take an action that may or may not be in their best interest."

That definition may seem general, but that's because social engineering attacks take a multitude of forms, both using a computer and in the physical world. With the above definition in mind, it becomes apparent that almost every single security incident starts with at least some kind of social engineering.

- Phishing attacks attempt to get unsuspecting users to click on a link, download a file, or respond with personal details.
- Phone spoofing, or "vishing," can involve being called by a scammer, or a scammer placing the call in an attempt to glean personally identifying information or resetting a password.
- Baiting attacks involve exploiting someone's curiosity to get them to something an attacker wants, like plugging in a found USB stick that then injects malware into a network.

- Pretexting, named not for sending an SMS message but rather for the act of presenting oneself under a false pretext, involves things like dressing in a delivery service uniform to sneak past guards, or "walking briskly and carrying a clipboard."
- SMS spoofing can also be used to convince smartphone users to call a number set up to harvest data, steal bank account information, etc.

All of these techniques present a false front that convinces someone to do something, unwittingly, against their best interests.

Social engineers don't need to be computer scientists, either: It's entirely possible to be a successful social engineer if you have a quick wit, good soft skills, critical thinking abilities, can think like a bad guy, and do good research.

Social engineering is used by hackers, penetration testers, fictional action heroes, spies, and con men. Even well-meaning people socially engineer situations to accomplish positive goals--for instance, I assume anyone with a child has fibbed to get their kid to do what they want.

In terms of cybersecurity, social engineering can cost businesses reputations, governments their secrets, and individuals hundreds of thousands of dollars.

WHAT ARE REAL-WORLD EXAMPLES OF SOCIAL ENGINEERING ATTACKS?

Real-life examples of successful social engineering attacks abound, and we can go well into history to find examples of actual social engineering tricks, like those perpetuated by Victor Lustig, who posed as a French official and successfully sold the Eiffel Tower for scrap--multiple times.

But there's no need to go back into the analog age to find examples of successfully run social engineering tricks--there are plenty to choose from.

- In late February 2020, an unknown party successfully conned Shark Tank investor Barbara Corcoran out of nearly $400,000 by sending a phishing email with a fake renovation invoice in it using an email nearly identical to her assistant's.
- Spear phishing campaigns against the Democratic National Committee and the Clinton Foundation made off with troves of documents that may have influenced the 2016 presidential election, many stolen by impersonating Gmail officials and asking targeted individuals to reset their passwords using a malicious link.

- A European Toyota subsidiary was conned out of over $37 million USD through a BEC attack that resulted in banking details being changed and massive deposits being sent to cybercriminals.
- In 2015, a 15-year old British boy successfully vished his way into the accounts of CIA chief John Brennan, FBI director Mark Giuliano, and US Homeland Security secretary Jeh Johnson, stealing government documents, resetting personal iPads, and displaying taunting messages on Johnson's home television.
- A pair of security researchers created a fake online persona named Emily Williams, and with it managed to con their way into government networks, gain access to a corporate-owned laptop, and got access to VPNs and other secured resources.

These are only a few examples of social engineering attacks against real targets that had real consequences, and there are many more where that came from.

A quick Google search will net you dozens of stories about successful social engineering attacks, and with good reason: An estimated 98% of cyberattacks are launched using social engineering, making it far more of a threat than direct exploit targeting by hackers.

WHO IS AT RISK FOR A SOCIAL ENGINEERING ATTACK?

There's no two ways about it: Everyone is at risk of being targeted for a social engineering attack, and those attacks are getting more successful. Numbers from security research firm CyberEdge indicate that more attacks are succeeding year over year, up to 78% in 2019.

Social engineering is successful because it's so insidious. It preys on people's desire to help, or inherent trust granted when an email comes from someone who is perceived to be a supervisor, government official, or other authority figure.

Social engineering attacks take a variety of forms, like phishing emails, watering hole websites that mimic legitimate pages, and low-tech attacks like calling a help desk and tricking them into resetting a user's password.

- If you have access to a secure system, you're a potential target.
- If you work in the public eye, your name is known, and your contact information is easily found, you're a potential target.
- If you're wealthy, you're a potential target.
- If you work at a help desk or in a call center, you're a potential target.

- If you have any kind of personal information locked behind a password on the internet, you're a potential target.

In short, everyone can be targeted by a social engineer, whether you fit into one of the above categories or not. If you're part of our modern, internet-connected world, you need to be on guard for social engineers, in person, on the phone, and through indirect digital forms of communication.

HOW CAN I PROTECT MYSELF AGAINST SOCIAL ENGINEERING HACKS?

There are a lot of different angles social engineering attacks can take, so there are various things individuals and organizations need to do to protect themselves.

Be aware of what information you make available

Lots of social engineering attacks rely on knowing something about the intended target, and where better to gather that information than on social media?

IBM chief people hacker Stephanie Carruthers warns against posting sensitive information in public spaces: "Think about what you're posting. Do you really need to tell everyone that you're going on vacation?"

Something as seemingly innocuous as posting a photo of your child's birthday party gives a social engineer several security question attempts, PIN tries, and password guesses. Going on vacation, talking about favorite books and movies, discussing where you met a partner--all of these things are information you're giving away freely to attackers when you post publicly online.

To be safe, ensure your profile is either devoid of this kind of information and designed to be public facing, or locked down so that strangers can't see what you don't want them to.

Carruthers also advises people to check websites for personal information that may be publicly available, like addresses, phone numbers, etc., and request it be removed. Also, subscribe to websites like haveibeen-pwned, which collates data from breaches into a searchable format and notifies users when their information is discovered online.

Do everything you can to make sure your personal information isn't available, and to be extra safe be sure you're not using easily guessed information as passwords, security answer questions, or password reminders.

Educate your users

IT departments should be sure that email filters are in place to block spam email and phishing attempts, and all

employees should be trained to recognize phishing and other forms of social engineering. Make sure people know what red flags to watch for, especially if they are in a position to interact with potential social engineers.

Users should be trained to question anyone they don't recognize, and to be questioned if they're in an area they don't usually go--questioning or being questioned can be uncomfortable, but it's better to demand answers and get to know a coworker than to be responsible for letting a hacker walk right in the front door.

Put good policies in place

Put policies in place that will make it harder for a social engineer to break in, digitally or physically. Ensure passwords are long and complicated, force users to change passwords on a regular basis, require two-factor authentication, block users from doing certain things while out of the office, and ensure tight control of physical access tools, like RFID cards and passcodes.

It's also a good idea to consider hiring a security firm to perform a social engineering audit of your organization. An audit can tell you if you're prepared for an attack, where your weak spots are, and how to be safe against social engineers who actually want to do you harm.

It can seem insurmountable when faced with potential spoof phone calls, phishing emails, smooth-talkers, and disguised attackers, but it isn't: It just takes knowing what sensitive information is, controlling how it's shared, and being aware when something isn't quite right.

These strategies won't eliminate your chances of being a social engineering victim. Not to be a doomsayer, but there's nothing that can truly prevent a determined and skilled social engineer.

By putting up every possible barrier to entry you can significantly mitigate your chances of being a victim: Think of fighting social engineering less like plugging every possible hole, and more like making an attack more of a hassle than it's worth. There's always another mark out there, and it's everyone's job to make sure they, their friends, and their coworkers don't get fooled.

CREDITS

Editor In Chief
Bill Detwiler

Editor In Chief, UK
Steve Ranger

Associate Managing Editors
Teena Maddox
Mary Weilage

Editor, Australia
Chris Duckett

Senior Writer
Veronica Combs

Senior Writer, UK
Owen Hughes

Editor
Melanie Wolkoff Wachsman

Staff Writer
R. Dallon Adams

Associate Staff Writer
Macy Bayern

Multimedia Producer
Derek Poore

Staff Reporter
Karen Roby

TechRepublic

ABOUT TECHREPUBLIC

TechRepublic is a digital publication and online community that empowers the people of business and technology. It provides analysis, tips, best practices, and case studies aimed at helping leaders make better decisions about technology.

DISCLAIMER

The information contained herein has been obtained from sources believed to be reliable. CBS Interactive Inc. disclaims all warranties as to the accuracy, completeness, or adequacy of such information. CBS Interactive Inc. shall have no liability for errors, omissions, or inadequacies in the information contained herein or for the interpretations thereof. The reader assumes sole responsibility for the selection of these materials to achieve its intended results. The opinions expressed herein are subject to change without notice.

Cover Image: Tero Vesalainen, Getty Images/iStockphoto