CYBERSECURITY

BACK STAGE PASS

SOCIAL ENGINEERING

Staying Alert for Subtle Scams

Many of us admire when a clever criminal uses old-school confidence tricks, scams, and manipulation to achieve their ends—at least, when it happens in books, movies, and TV shows. But real-life attacks are seldom glamorous, and they can have serious consequences.

Criminals often try to trick employees into giving them access to sensitive information or valuable assets, such as trade secrets, financial documents, and customer information. Organizations lose billions of dollars each year to these schemes.

The psychological tricks criminals use are sometimes known as *social engineering*.

What Is Social Engineering?

You can think of social engineering as an umbrella term that covers a variety of tactics that manipulate our human nature and instincts. Some are age-old tactics that cybercriminals have adapted to use online, in email, and on social media.

While these tricks are subtle and effective, they're not superpowers. A social engineer doesn't need otherworldly powers of persuasion to convince someone to ignore or disable security measures. Often, they rely on creating a sense of urgency.

Let's say that you receive an email, and the urgent tone or content makes you feel that you should ignore a security warning and open a malicious attachment. This is one example of how an attacker might use social engineering to manipulate you into installing malicious software (malware).

Another common approach is to build familiarity and trust. An attacker may research an organization's routines, processes, and cultural norms to establish credibility. Then, they may be able to persuade an employee to transfer money to the scammer's account instead of a legitimate account.

An Attacker's Arsenal

A successful social engineering attack often involves a combination of tactics. Here are some common examples:

- **Phishing emails and texts** – Fraudulent emails and text messages can entice, trick, or scare a person into clicking malicious links or providing confidential information.
- **Researching targets online** – Scammers use social networks to gather personal details, and may try to impersonate a legitimate connection online.
- **Voice phishing (vishing)** – Phone calls provide direct access for scammers to ask for confidential information.

While social engineering tricks are subtle and effective, they're not superpowers.

BANK OF THE WEST
BNP PARIBAS

TIPS FOR FAMILY AND FRIENDS

Social engineers target individuals as well as large organizations—and they aren't above small-time swindles. Here's some good advice to share with family and friends:

- **Be skeptical** – Don't blindly trust a stranger, a person on the phone, or the sender of an email.
- **Recognize when you're feeling pressured** – Scammers want you to act without thinking clearly, so they often try to create a sense of urgency.
- **Ask for ID** – If a stranger arrives at your office or home, ask for identification. Then, confirm the visit by contacting the vendor, service provider, or organization through a verifiable phone number (not a number from the visitor's business card).
- **Stay alert for shoulder surfers** – Don't let someone watch what you type or see your screen. Shield your PINs and passwords, particularly if you have to use these sensitive pieces of information in a public setting or at work when others are present.

SUBTLE	VISHING
URGENCY	TAILGATING
TRICK	MALWARE
HUMAN NATURE	CONVINCE
FAMILIARITY	DECEPTION
PHISHING	VERIFY
CREDIBILITY	TRUST

Find and circle all the words associated with social engineering hidden in the grid. The words are hidden in all directions.

- **In-person deception** – Scammers may visit their target locations, often using a false identity. They might pretend to be a vendor or contractor, a job applicant, or an employee.
- **Tailgating** – A scammer may try to follow another person through a secure entrance. They may pretend to have lost their badge and ask you to hold the door for them.
- **Shoulder surfing** – Scammers can steal passwords, access codes, PINs, and other important information just by observing you. A scammer typically tries to watch a user log into a system to learn their credentials, using a camera, software, or their own eyes.

Developing Your Own Skills

Remember: Social engineers don't have superpowers. You *can* learn to identify their attacks and help to protect yourself, your organization, and your friends and family. Here are a few tips to start building your own skills:

- Verify that people are who they claim to be, in person, via email, and on the phone
- Trust your instincts—if something seems odd, ask your manager for help
- Protect passwords and other secure data
- Never hold open secure doors for people you don't know

You can learn more about social engineering in your organization's security awareness training.

Activity Corner // Social Engineering Word Search

G	D	E	C	E	P	T	I	O	N	U	I	K	G
L	F	L	N	E	L	T	B	U	S	P	M	E	T
I	A	S	H	E	L	N	I	G	E	H	A	R	C
T	M	P	I	N	M	L	U	C	C	I	L	U	R
A	I	I	F	Y	E	M	N	G	N	S	W	T	E
I	L	L	U	W	P	N	G	T	I	H	A	A	D
L	I	A	O	U	T	S	M	R	V	I	R	N	I
G	A	S	U	R	A	C	U	U	N	N	E	N	B
A	R	B	I	G	K	N	Y	S	O	G	T	A	I
T	I	A	M	E	C	C	E	T	C	F	V	M	L
I	T	E	G	N	I	H	S	I	V	E	Y	U	I
N	Y	T	C	C	R	V	R	L	N	R	F	H	T
G	D	T	F	Y	T	N	G	G	A	M	I	M	Y
I	B	Y	F	I	R	E	V	I	R	C	C	A	E

BANK OF THE WEST
BNP PARIBAS