-Phishing, Smishing, Vishing, and Quishing-

The Human Element in Cybersecurity

Cybersecurity Awareness Month 2025

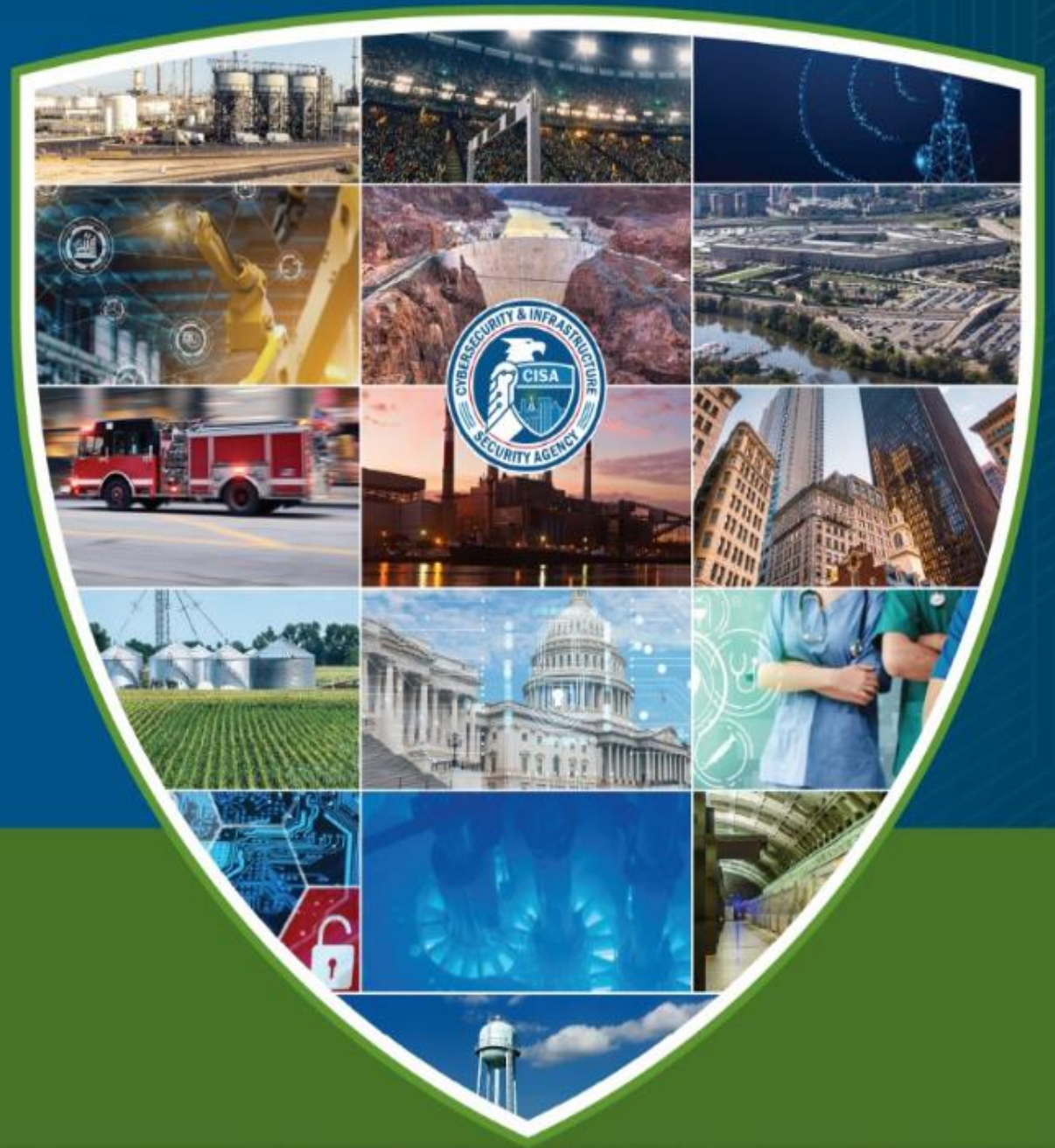
Presented by the

Homeland Security Human Factors Institute™
A Division of Behavioral Science Applications LLC
Behavioral Risk Management Advisors

Welcome

BUILDING A

CYBER STRONG AMERICA



CYBERSECURITY AWARENESS MONTH

OCTOBER 2025

About the Instructor

Steve Crimando, MA, CTM

Founder & Principal – Behavioral Science Applications LLC
Director - Homeland Security Human Factors Institute™

35+ year emergency behavioral health clinician, educator & crisis responder

Certified Threat Manager (CTM) - Association of Threat Assessment Professionals

Certified Master Trainer - U.S. Department of Homeland Security-National Threat Evaluation & Reporting (NTER) program

Consultant/Trainer for the

N.J. Statewide Threat Assessment Team (NJ STAT)
U.S. Department of Homeland Security - FEMA & NTER
U.S. Department of Justice - FBI Joint Terrorism Task Force
U.S. Health & Human Service - Substance Abuse Mental Health Services Administration
U.S. Department of State-Foreign Service Institute
U.N. Operational Support Section - Special Situations Unit

Our Approach

During this program, we will be employing an approach known as ***"Operational Psychology"***

Operational psychology typically involves the application of the behavioral sciences to national security, law enforcement, and military operations.

It is the use of clinical, cognitive, and social psychological concepts for their tactical value.

It can help us improve our ability to rapidly form **accurate behavioral assumptions,** which can give us critical strategic and tactical advantages in managing various operational risks.

Today we are focused on the human element in cybersecurity threats.

Cybersecurity Risks are Everywhere

Nearly one third of new homes built in the U.S. included smart home technology integrating connected devices and automation systems—such as smart thermostats, lighting, security systems, and voice assistants—into newly constructed homes.

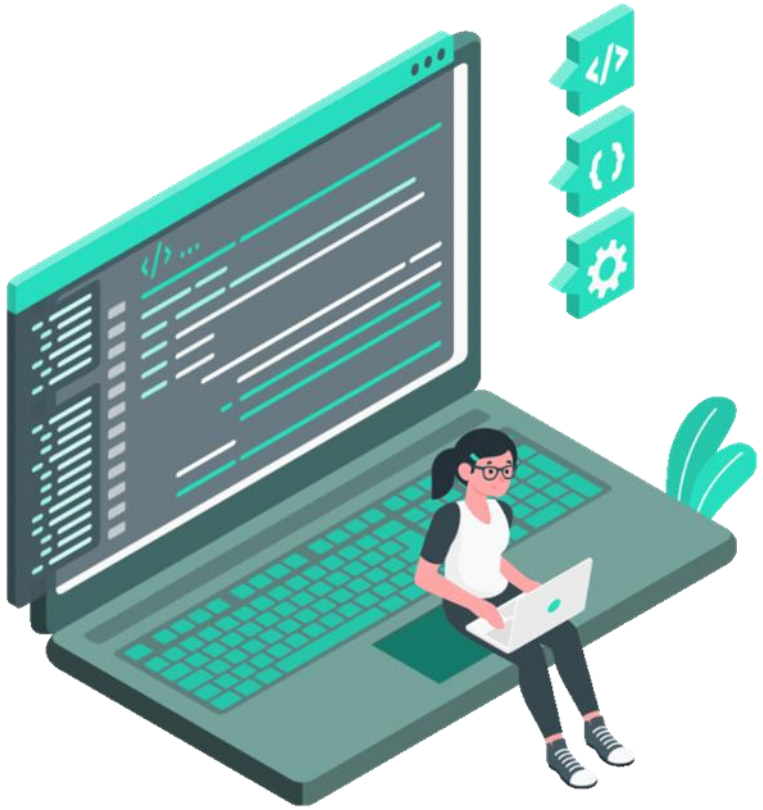
What Is Cybersecurity?

Cybersecurity is the protection of computer systems and networks from attacks by malicious actors that could cause unauthorized information disclosure, theft, or damage to hardware, software or data.

We will also address scams and exploitation perpetrated in the cyber-environment.

Wherever there is technology, there needs to be cybersecurity.

A Two-Part Solution [1]



The challenge of dealing with cybersecurity is complex.

Human factors and the human-computer interface are the two central components of cybersecurity.

Technology alone will not prevent cybercrime, neither will people.

People alone cannot be relied upon as a last line of defense in an organization's cybersecurity strategy.

A Two-Part Solution [2]

Because **threat actors understand human behavior,** they know how to manipulate it to achieve their goals—stealing money and valuable information from enterprises and small businesses alike.

These criminals use various types of social engineering to complete their schemes, relying on urgency and name recognition to trick their victims.

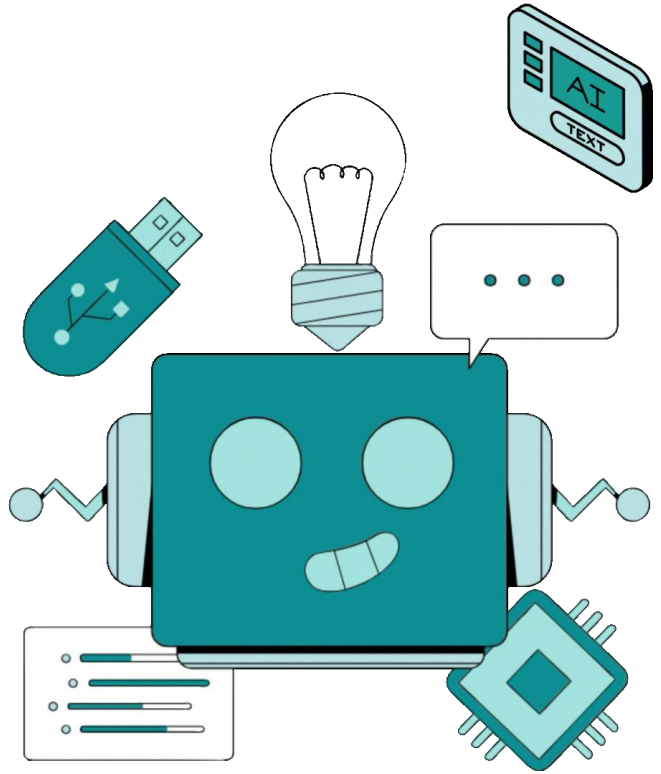
Why is it Important?

At Work | Implementing cybersecurity best practices helps protect intellectual property and other sensitive data, as well as networks and systems that support your operations.

For both government and private entities, developing and implementing tailored cybersecurity plans and processes is key to safeguarding operations and protecting critical infrastructure.

At Home | In today's hyperconnected world, the home is no longer just a private space—it's a digital hub. From smart devices and personal data to remote work and online banking, our households are rich targets for cyber threats.

Cybersecurity at home protects not only sensitive information but also the integrity of our daily lives. A single breach can compromise finances, privacy, and even physical safety.



The Weakest Link

Research shows humans have always been the weakest link in cybersecurity.

In order to truly protect your employees and organization, professionals across a range of disciplines must understand human behavior and what this means when it comes to social engineering.

It’s only by recognizing the social engineering threat that we can find ways to prevent it.

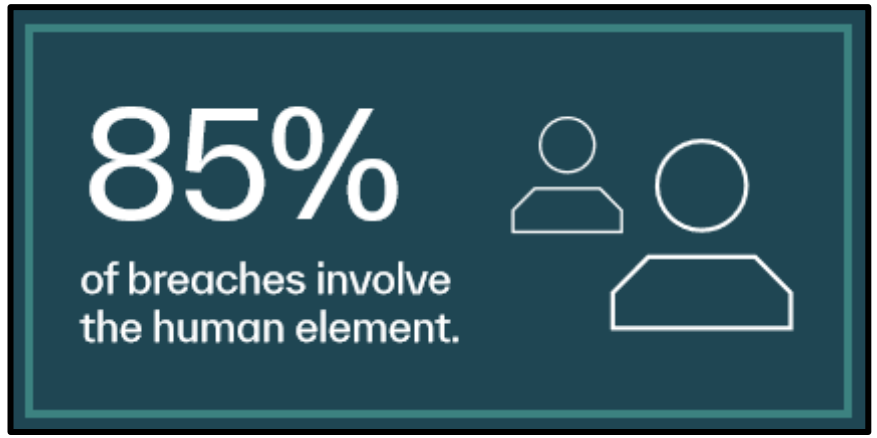
Human Behavior:
The Problem & the Solution

Cybersecurity is largely a behavioral concern; therefore, a component of any mature cybersecurity program is attention to human factors.

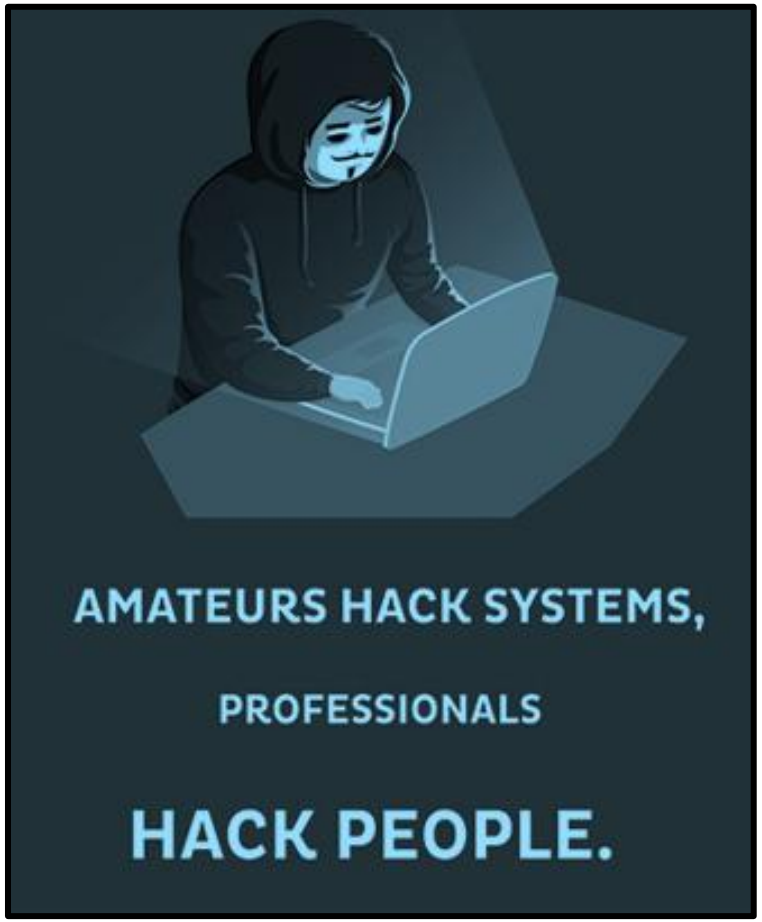
Research has consistently shown that **people are the weakest link** in both physical and cybersecurity.

Breaches happen primarily due to social engineering attacks which target us at work and at home.

What people do and don't do makes a huge difference in cybersecurity. Understanding why they do and don't do certain things can help us develop more effective solutions.



Understanding the Challenge



The strongest security network in the world is only as good as the human with the password.

Getting users to be attentive and adhere to security practices can be quite difficult.

Things as simple as clicking on a bad link, opening the wrong email attachment, or using an unsecured USB drive can be devastating to network security.

But most spending on cybersecurity continues to be on technology, when the problem is largely behavioral.

Breaking Rules

Accidentally or maliciously, people break cybersecurity rules from password policies to data storage and data exfiltration.

Employees can be unfocused, unaware, or unfamiliar policies or the consequences of poor cybersecurity practices.

For example, they may not understand the risks of emailing company information to their personal email account to review or print at home.

Making Mistakes

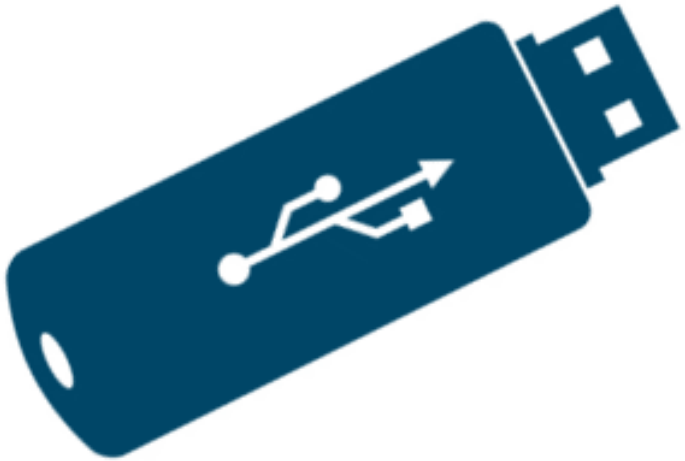
Simple typos, clicking on unknown links, or plugging in an unknown USB drive—for a number of reasons, people make mistakes.

People are pretty bad at telling the difference between a real website or email, and fakes.

In fact, 43% of employees say they've made a mistake at work that compromised cybersecurity. Some of these can have severe consequences.

Mistakes can result in penalties and fines,
a loss of customer trust, and reputational damage.

Individuals can suffer and may lose their jobs.



Increased Cyber Risk in the Work-from-Home

The pandemic greatly increased usage and reliance on the internet, giving hackers more opportunities to scam people with malware and phishing attacks.

One security research survey has found that that **37% of employees working remotely from home, have faced an increased risk of phishing attacks** since the pandemic.

Social Engineering | Human Hacking

Social engineering is any form of cybercrime based on impersonation and is sometimes referred to as **pre-texting.**

As part of the attack, a cybercriminal tries to convince his victim to send money or provide valuable information or access to a service or system.

The method is typically via email, but can also occur across texts, chat messages, and phone calls.

Social engineering scams can also be completed in person, but that method represents greater risks of detection for the criminal.

These attacks can be completed in a variety of ways, but the most popular version occurs when the attacker pretends to be a trusted person. They then convince the target to follow their instructions.

In doing so, the target unwittingly creates an opportunity for the attacker to steal money or compromise security.

Deception & Pretexting [1]

Hackers can and do impersonate internal and external contacts to manipulate people for malicious purposes.

An attacker obtains information through a series of cleverly crafted lies. The scam is often initiated by a perpetrator pretending to need sensitive information from a victim so as to perform a critical task.

The attacker usually starts by establishing trust with their victim by impersonating co-workers or family members, police, bank and tax officials, or other persons who have right-to-know authority.

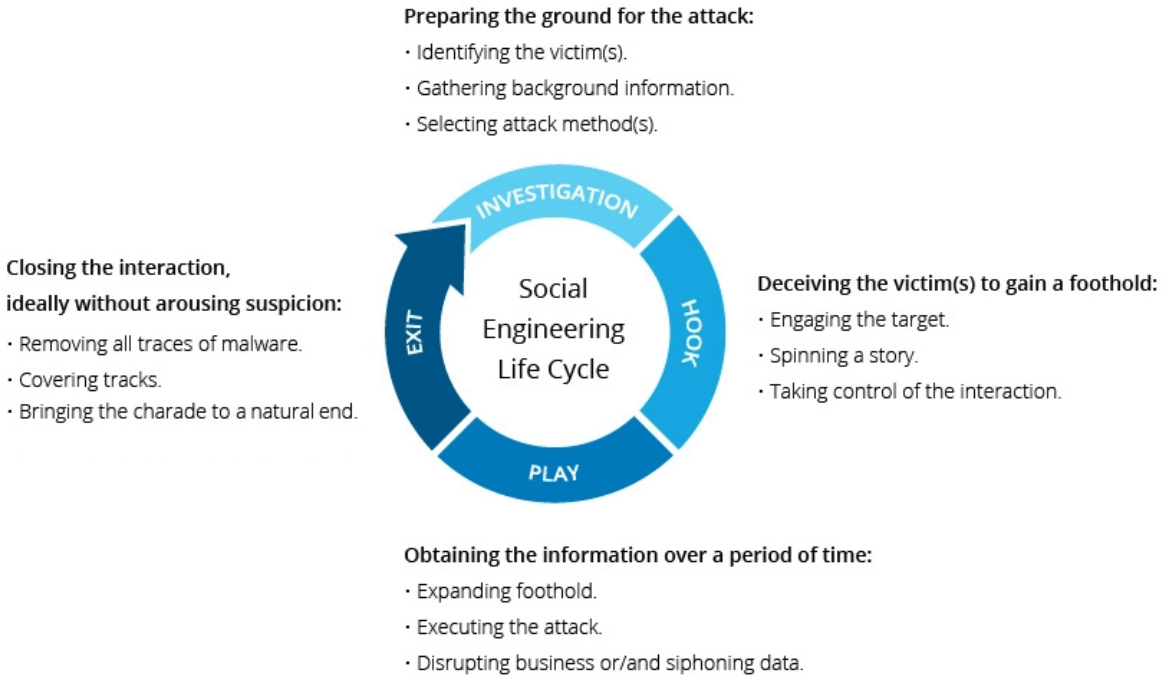
The pretexter asks questions that are ostensibly required to confirm the victim's identity, through which they gather important personal data.

Deception & Pretexting [1]

All sorts of pertinent information and records are gathered using this approach, such as social security numbers, personal addresses and phone numbers, phone records, staff vacation dates, bank records and even security information related to a physical plant.

Deception is especially dangerous in that it relies on human error, rather than vulnerabilities in software and operating systems.

Mistakes made by legitimate users are much less predictable, making them harder to identify and thwart than a malware-based intrusion.



Hackers Understand People

Unlike the stereotypical portrayal of hackers by Hollywood, they often have a very keen understanding of human nature.

Hackers understand the power of the psychological factors, like fear, ego, or not wanting to miss an important opportunity or task, especially for someone of authority.

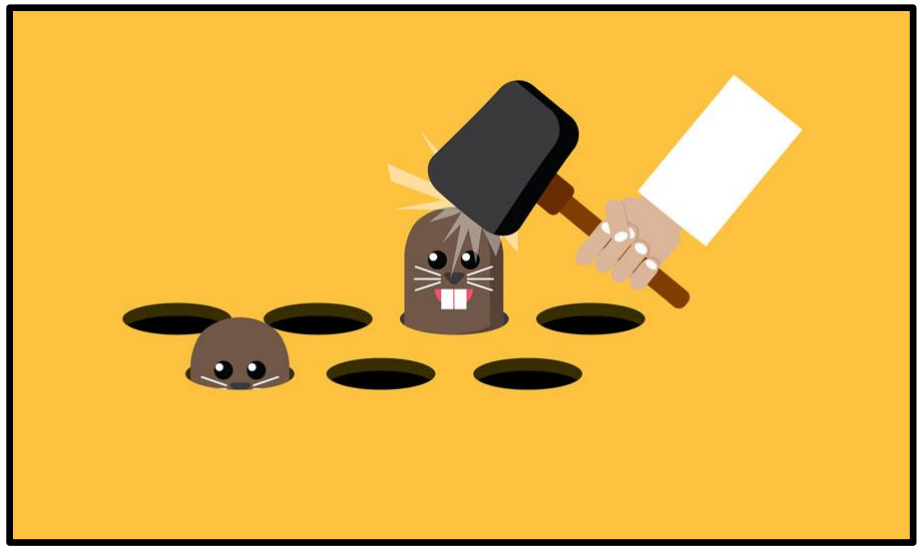
At the same time, they effectively capitalize on situational factors, like social, political, and economic stress, as well as concerns about personal health and safety.

Social Engineering Tactics

Cybersecurity often resembles a game of Whac-a-Mole, as attackers continue to invent new methods to thwart constantly-evolving cybersecurity.

Attackers are not only cognizant of the vulnerabilities in networks and systems, but also of the changing attitudes and behaviors of their targets.

They understand how people may behave differently at different times of the day or year, as well as in response to the changing use of technology, or the societal impacts of the pandemic.



Phishing | Spear Phishing | Whaling [1]

Phishing

A social engineering attack conducted via email. Phishing attacks tend to be **broad and may target hundreds of people** across multiple organizations with the same message.

Spear Phishing

Similar to a phishing attack, this email or electronic communications scam is **targeted towards a specific individual,** organization, or business. Spear phishing is more targeted than phishing and typically contains specific information that the target would expect to receive.

Phishing | Spear Phishing | Whaling [2]

Whaling

A phishing attack targeting a corporate executive or government official.

This attack type is called whaling because the targets tend to be *"big whales"* within an organization, with access to large funds or extra sensitive information.

72%
of whaling attackers pretended to be the CEO, while 36% were attributed to the CFO.

Phishing | Spear Phishing | Whaling [3]

Each of these social engineering methods involves some type of impersonation, either of a person or a brand.

The social engineer often uses sophisticated techniques to make their impersonations more convincing, including making email addresses, URLs, and websites look genuine to fool their targets.

They do this to manipulate their targets through **normal human emotions and concerns,** playing on urgency and creating pressure to convince people to do something before they've had time to think it through.

Recognize and Report Phishing [1]

How can you tell if a message is phishing?

A tone that's urgent or makes you scared

Ex: "Click this link immediately or your account will be closed."

Sender email address doesn't match the company it's coming from

Ex: Amazon.com vs. Amaz0n.com

Unexpected communications such as an email or attachment you weren't expecting

Requests to send personal info

Legitimate organizations don't ask for personal information through email or an unexpected call.

Misspelled words, bad grammar and odd URLs

Be aware that AI will make spotting these more challenging—stay diligent.

Recognize and Report Phishing [2]

What should you do if you spot a phish?

DO

Verify that the communication is real and contact the sender directly through known phone numbers or emails.

Report it to your IT department or email/phone provider.

Use email filters. Many email services have filters that can help prevent phishing messages from ever reaching your employees' mailboxes.

DELETE IT.

DON'T

Don't click any links you don't trust, even "unsubscribe" (just delete).

Don't click any attachments you were not expecting or recognize.

Don't send personal info online or share over the phone.

Smishing

Smishing is a type of phishing attack that uses SMS (text messages) to trick individuals into revealing sensitive information or clicking malicious links.

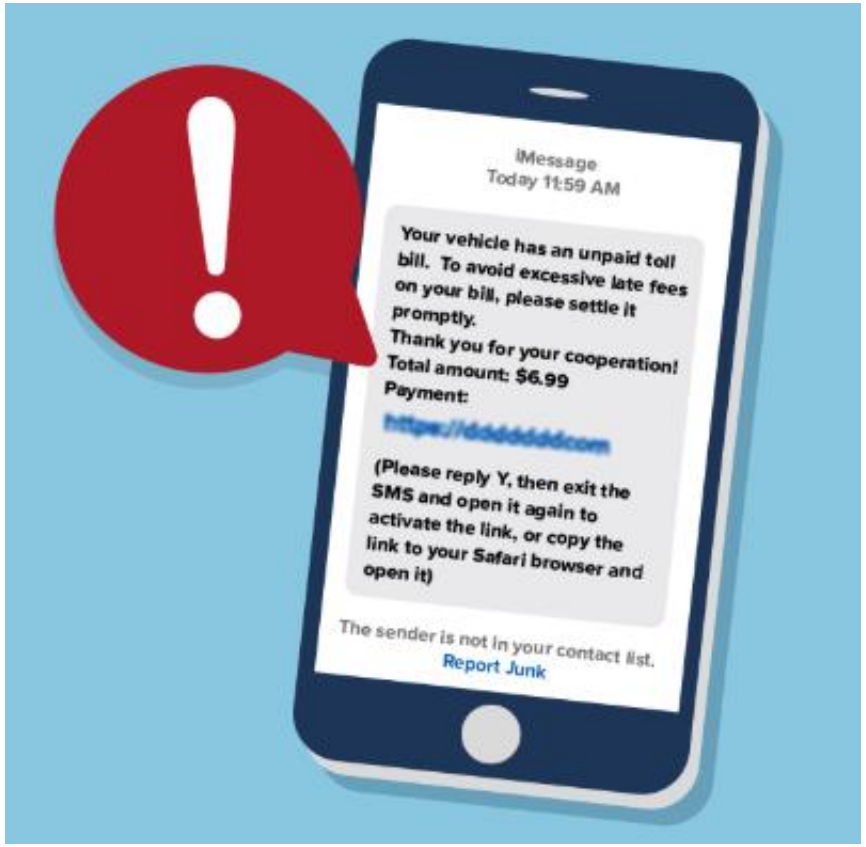
The term combines “SMS” and “phishing.”

These messages often appear to come from trusted sources—banks, delivery services, or government agencies—and may:

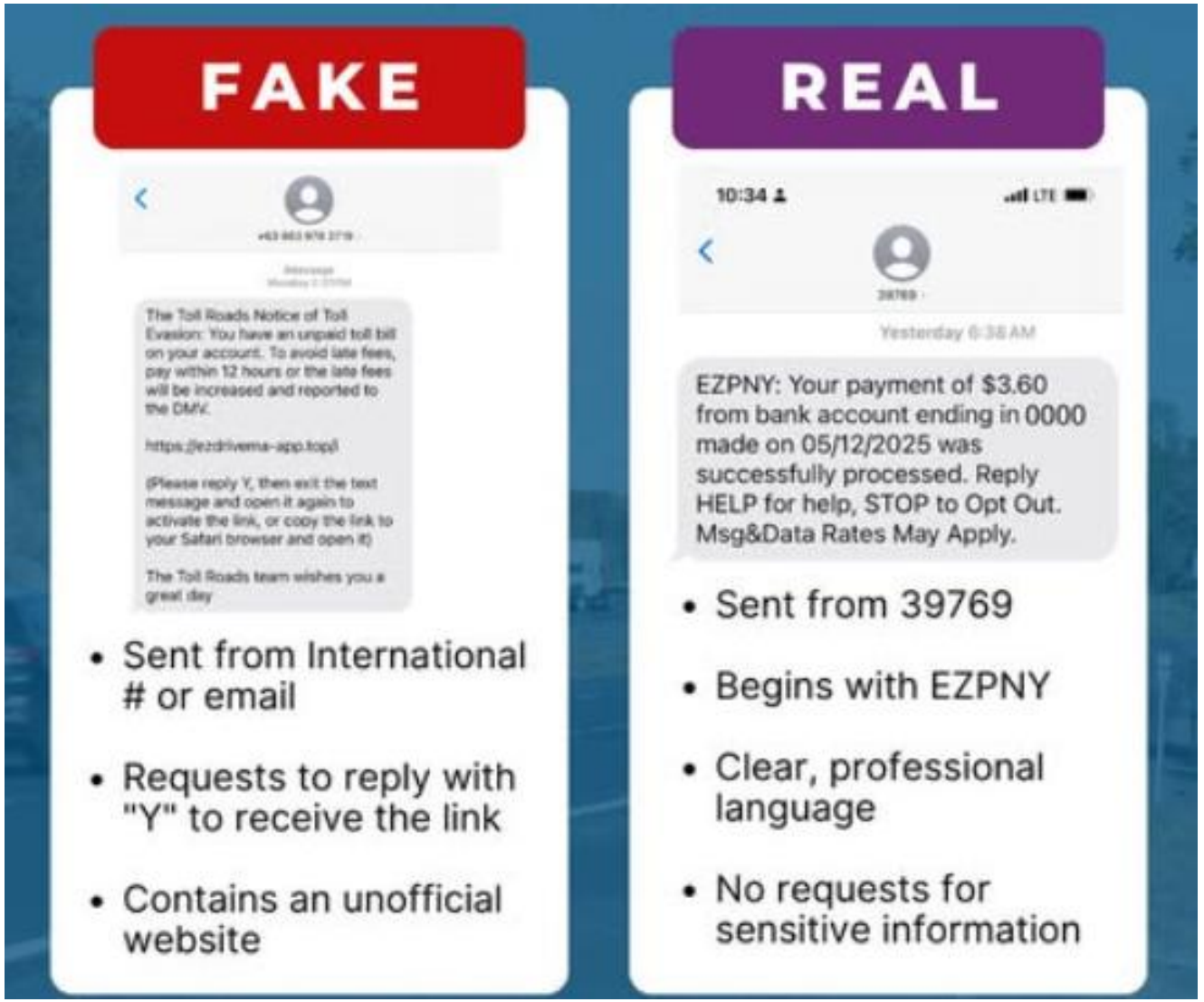
Urge immediate action (e.g., “Your account is locked. Click here to verify.”)

Contain links to fake websites designed to steal credentials

Ask for personal information like passwords, credit card numbers, or social security numbers



How Can You Tell?



How to Respond to a Smishing Attack [1]

Do Not Click or Reply

Avoid tapping any links or responding to the message.

Even a simple reply like “STOP” can confirm your number is active.

Take a Screenshot

Document the message for reporting and investigation.

Include the sender’s number and timestamp.

Block the Sender

Use your phone’s settings to block the number.

This helps prevent future messages from the same source.

How to Respond to a Smishing Attack [2]

Report the Attack

Forward the message to 7726 (SPAM)—a free reporting service supported by most carriers.

Notify your organization's security team if the message targets work-related data.

Delete the Message

Once documented and reported, remove it from your device.

This reduces the risk of accidental interaction later.

Monitor for Fallout

Watch for signs of identity theft or account compromise.

Consider updating passwords if you clicked a link or entered information.

Vishing

Vishing is short for "voice phishing"—a type of social engineering attack where scammers use phone calls to trick individuals into revealing sensitive information.

Unlike email or text-based phishing, vishing relies on verbal manipulation. Attackers often impersonate trusted entities such as banks, tech support, government agencies, or even company executives. Their goal? To extract personal data, financial details, or login credentials.

Common tactics include:

- Imminent risks ("Dad, this is Susie! I'm in trouble, I need your help!")
- Urgent threats ("Your account will be suspended unless you act now")
- Fake tech support ("We've detected a virus on your computer")

Spoofed caller IDs to appear legitimate

What to Do [1]

Do Not Engage

Hang up immediately if the call feels suspicious or demands urgent action.

Avoid sharing any personal, financial, or login information.

Verify the Caller

Contact the organization directly using official contact information (e.g., bank website, company directory).

Never trust caller ID alone—spoofing is common.

Document the Incident

Note the time, phone number, and content of the call.

Save any voicemails or call recordings if available.

What to Do [2]

Report the Incident

Notify your organization’s security or compliance team.

Report to the FTC (in the U.S.) via reportfraud.ftc.gov

Inform your phone carrier—they may block the number or investigate.

Monitor for Fallout

Watch for signs of identity theft or account compromise.

Consider placing fraud alerts or credit freezes if sensitive data was exposed.

Quishing

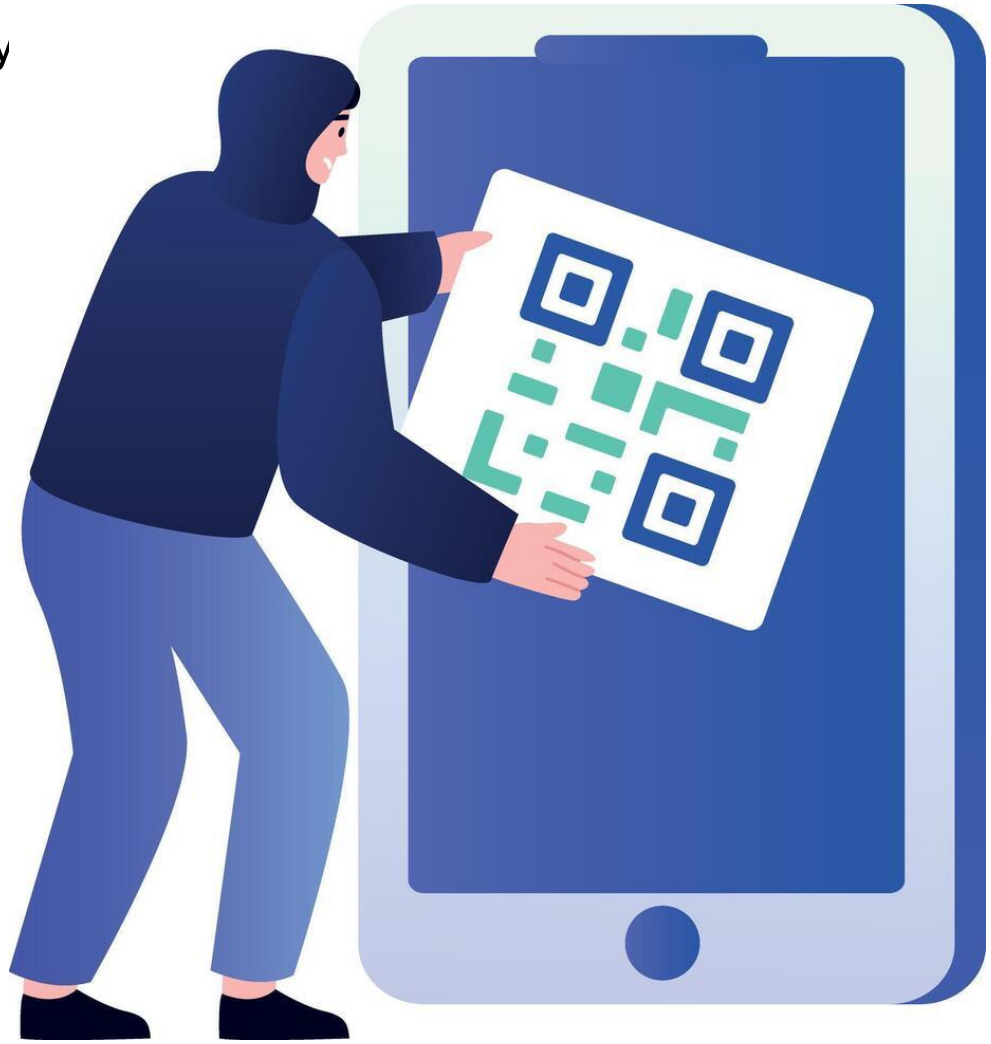
Quishing—short for QR phishing—is a cybersecurity threat where attackers use malicious QR codes to trick individuals into visiting harmful websites or downloading malware.

Attackers generate a QR code linked to a fraudulent site or malicious download.

The code is embedded in emails, flyers, social media posts, or even physical objects.

Victims scan the code with their phone, often without verifying the source.

The site may prompt users to enter sensitive information (e.g., login credentials, financial data) or install malware.

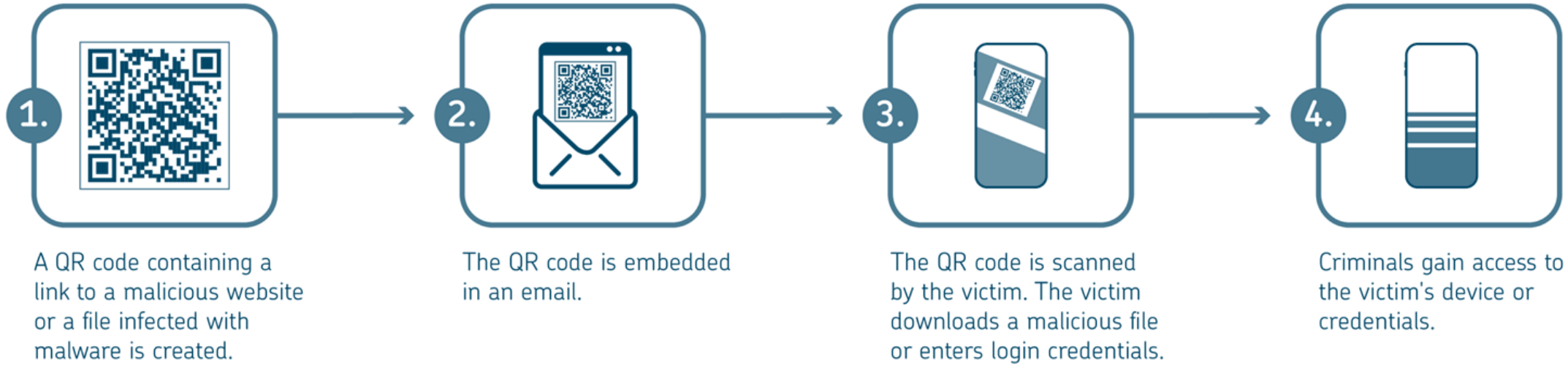


Why is Quishing Dangerous?

QR codes bypass many traditional security filters, especially in email.

They exploit user trust and convenience—people scan without thinking.

Quishing can lead to identity theft, financial fraud, or ransomware attacks.



Defending Against Quishing

Verify the source before scanning any QR code.

Avoid entering personal info or downloading apps from QR-linked sites.

Use mobile security tools and educate teams on QR-based threats.

Four Essential Behaviors to Stay Safe Online

Update software

Use strong passwords and a password manager

Turn on multifactor authentication (MFA)

Recognize and report phishing

Hacker Tactics | Authority

An attacker may represent themselves as an authority figure, such as an executive or an in-house IT specialist, to create the impression that their directions must be followed and not questioned.

There is a natural human tendency for humans to avoid pain, and attackers know that people are more likely to follow instructions when they come from someone in power.

Hacker Tactics | Intimidation

Again, using fear as a lever, the attacker informs or implies that there will be negative consequences if certain actions are not performed.

Consequences could include subtle intimidation such as *“I’ll tell your manager”* and more serious results like, *“The whole system will go down if you don’t install this patch!”*

Social engineers are experts in creating a sense of impending doom.

Hacker Tactics | Consensus-Social Proof

People seek confirmation and will typically do things that they see or believe other people are doing.

The attacker might try to convince their target that everyone else has already taken a certain action, and therefore, the target should do so as well.

Hacker Tactics | Scarcity

An attacker can create an **illusion of scarcity** by telling their would-be target that there is a limited opportunity to take a specific action.

Human nature is such that when we believe things will become less accessible, we can be compelled into action.

This concept is often used in sales by suggesting that an opportunity is available for ***"a limited time only!"*** but can also be used by attackers to convince their targets to take quick action.

Hacker Tactics | Urgency

By **creating a time-imperative,** an attacker can create the impression that the target must act quickly or by failing to do so, there may be dire consequences.

For example, if the target does not update their password in the stated time frame, they will lose their ability to access the network.

In addition to using fear as a motivator, a tight timeline for taking action increases stress, decreases the opportunity for people to think the situation through, and increases the likelihood of an error.

Hacker Tactics | Familiarity-Liking

People typically follow the lead of other people whom they like. If we like someone, we are more likely to do what the person asks.

Social engineers may attempt to build rapport with the victim to build a relationship before launching the attack.

Attackers also use this tactic after compromising an account, taking advantage of an established relationship to convince the target to take an action they normally would not take.

Alone or In Combination

These common social engineering strategies and techniques are not mutually exclusive.

They can be used in combination, making them less obvious and potentially more confusing for their victims.

There are endless variations on these themes that are used every day to trick people into complying with the will of the social engineer.

AI & Cyberthreats

AI is providing tools to scammers that can easily be used to fool even the most sophisticated security professionals.

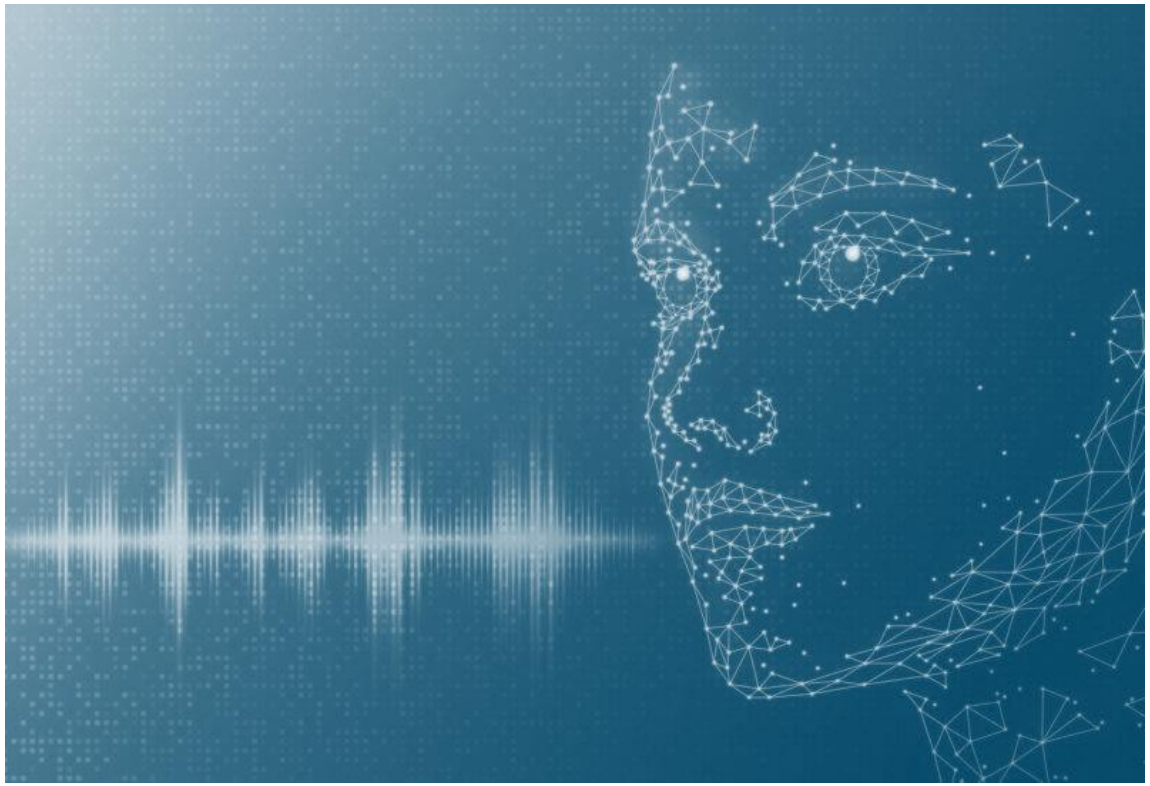
The classic technique of social engineering involves deceptive practices, such as impersonation or manipulation of trust, to extract personal and confidential information from targeted individuals.

As AI tools increase in potency and accessibility, social engineering attacks are now significantly more personalized, effective, and scalable.

Gen AI Risks

The computational power of AI can create and spread information fast and far-reaching ways.

Two of the main risks associated with AI are the potential for AI generated voice and video impersonation.



Deep Fake Voice Replication

AI-generated voice scams—especially those mimicking loved ones in fake kidnapping scenarios—are deeply manipulative and emotionally charged.

Help!

"I'm in jail and need bail money!"

"I owe someone money, and they are going to hurt me!"

"I've been kidnapped!"

All this in the voice of your loved ones and also used a *"spoofed"* phone number making it feel very real!

What to Do

Be cautious about posting voice recordings online (e.g., videos, podcasts).

Review privacy settings on social media to restrict access to audio content.

Have conversations with those in your circle and develop a verification protocol.

Create a unique, hard-to-guess phrase known only to close family members.

Use it to verify identity during any emergency call or message.

If you receive a distressing call, don't act immediately—Hang up and double check.

Try to contact the person directly through another channel.

Ask questions only your loved one would know—especially the safe word.

Report and Document: Notify law enforcement and your phone carrier.

Save call logs, voicemails, and screenshots for investigation.

Stay calm, verify, and never send money or personal data without confirmation.

Gen AI Deep Fake Images & Videos

AI Deep Fake imagery is increasingly realistic and difficult to distinguish from real images.

These images can be used for a variety of malicious purposes ranging from personal to corporate reputational harm, to spread disinformation that can incite violence to self and others, and to create larger societal chaos.

Deepfake Pornography & Suicide Risk

If a child is a victim of AI-generated, image-based sexual abuse, they may experience **humiliation, shame, anger, violation, and self-blame.**

These outcomes can contribute to immediate and continual emotional distress, withdrawal from family and school livelihoods, and challenges with sustaining trusting relationships.

Some cases can lead to self-harm and suicidal thoughts. If deepfakes are passed around a school community or peer groups, the victim may be bullied, teased, and harassed; trauma is amplified each time the content is shared.

Source | Thorn BSG

Become Unscamable [1]

Human behavior is the key to cyberthreats and protecting against them.

Developing a scam-proof mindset protects you from manipulation in everyday life. An online phishing email, a fake investment opportunity, or someone pushing a product that's *"just too good to pass up,"* all create windows of exploitation.

Three basic rules

If it came to you, test it.

If it flatters you, doubt it.

If it hurries you, stop it.

Become Unscamable [2]

This mindset nears but never touches paranoia, while creating discipline.

By assuming there's always another layer beneath what's being presented, you can avoid the traps that rely on trust, speed, and emotional reaction.

The result is

A reflexive pause,

A demand for context,

An instinct to ask questions others never consider.

Become Unscamable [3]

By slowing down, interrogating the details, and recognizing when something feels unnaturally polished or enticing, anyone can cut through the illusion.

The shift is subtle but powerful: instead of being pulled along by the scammer's script, you remain in control, dictating the pace and demanding clarity.

This shift in mindset, training yourself to look beneath the surface, turns everyday encounters into something you actively manage rather than something that manages you.

This training is based on recognizing three key indicators that's universally applicable.

Become Unscamable [4]

The [First] Indicator | You're Being Solicited

A scam nearly always starts the same way - you didn't seek it out; it came to you.

Remember, who initiates contact is often more important than what's being offered.

This means they've already selected you as a target—That alone is reason to be cautious.

Flag unsolicited contact as suspicious until you've stripped it down and examined its purpose.

The moment you didn't seek something out,
but it found its way to you, your alert level should rise.

Become Unscamable [6]

The [Second] Indicator | It's Too Lucrative

The next red flag is disproportionate reward. If the payout, discount, or benefit feels like it outweighs the input required, you're being baited.

Distrust anything that seems to give more than it takes.

When the balance between effort and reward feels lopsided, don't celebrate; scrutinize.

If the scales tilt too far in your favor, someone's tipping them for a reason.

Become Unscamable [8]

The [Third] Indicator | It's Too Good to Be True

This principle extends beyond money. Anything that feels frictionless, flawless, or perfect is suspect.

Perfection is not natural; it's engineered; the absence of flaws is itself a flaw.

When everything lines up too smoothly, it bypasses doubt and creates compliance.

When reward feels certain, risk is certain too.

Closing Thought

The effect of this conditioning is a mind that no longer takes things at face value.

Don’t live in constant suspicion; live in constant evaluation.

Separate signal from noise— benefit from bait—opportunity from entrapment.

Remember

Every scam is a performance.

Your job is to look behind the curtain.

Report Cyber Incident Information to CISA [1]

How do you report a cyber incident, or suspected cyber incident?

Use the online form at: cisa.gov/report

Report Cyber Incident Information to CISA [2]

What is cyber incident information sharing?

Cyber incident information sharing means reporting suspected or confirmed cyber incidents, system vulnerabilities or suspicious activity to CISA. In return, CISA shares threat intelligence, mitigation tips and technical assistance.

This sharing is **bidirectional**:

You share: Indicators of compromise, attack methods, timelines and system impacts.

CISA shares: Alerts, threat bulletins, mitigation advice, protective measures and tools to reduce risk.

Additional Resources

Cybersecurity Awareness Month

Report a Cyber Issue

Cross-Sector Cybersecurity Performance Goals

Cyber Resource Hub

Cybersecurity Training & Exercises

CISA YouTube Channel

BEHAVIORAL SCIENCE APPLICATIONS

Behavioral Risk Management Advisors

Office: +1.973.601.7222

Email: info@behavioralscienceapps.com

Web: www.behavioralscienceapps.com

www.facebook.com/bsacrisisintervention

www.linkedin.com/in/stevecrimando

https://www.youtube.com/channel/UCP06TtIfgTd4sT0glDFFpvw

