THE LAYPERSON'S GUIDE TO SECURITY SCAMS

What They Are, How They Work, and Tips for Protecting Yourself and Your Business

Because Security Starts with Awareness

The Layperson's Guide to Security Scams

Welcome to The Layperson's Guide

A plain-language companion for those who want to protect themselves & their business

Whether you're a business professional, healthcare worker, educator, or simply someone who uses a computer or phone — this guide was created for *you*.

Every day, scammers use increasingly sophisticated tactics to trick people into handing over sensitive information — passwords, account access, and entire identities. And while the terminology might sound technical, intimidating (and even a bit zany), the concepts behind these scams are surprisingly simple once explained in plain language.

That's exactly what this guide is meant to do.

In the pages ahead, as part of KSI's commitment to awareness, you'll find a growing glossary of the most common digital scams — from credential stuffing to deepfake fraud, and everything in between.

For each entry, we provide answers to:

- **What the scam is** *(a simple explanation)*
- **Why the scam works** *(how scammers fool people)*
- **Tips for protecting yourself** *

Above all, this guide is meant to empower you. When you know what to look for, it's much easier to stay safe, stay productive, and stay in control. We recommend that you keep this Guide nearby as a trusted reference to help recognize scams, understand how they work, and stay one step ahead of cybercriminals.

Thanks for reading!

Team KSI

Table of Contents

Navigation Tip: Click our interactive TOC to quickly get where you want to go

Credential & Identity Attacks

- Phishing
- Spear Phishing
- Whaling
- Smishing
- Vishing
- Business Email Compromise (BEC)
- Consent Phishing
- Credential Stuffing
- Password Spraying
- Man-in-the-Middle (MitM)
- Session Hijacking
- SIM Swapping
- Account Takeover (ATO)
- Replay Attacks

Social Engineering

- Pretexting
- Baiting
- Quishing
- Fake Online Stores
- Impersonation Scams

Malware-Driven Attacks

- Keylogging
- Ransomware
- Watering Hole Attacks
- Drive-by Download
- Trojan Horse / Spyware

Emerging AI-Enabled Attacks

- Deepfake Impersonation
- AI-generated Phishing Emails

Quick Reference Cheat Sheet

Credential & Identity Attacks

These attacks focus on stealing login credentials or tricking users into granting access to sensitive systems.

Whether it's through phishing emails, fake login screens, or deceptive app permissions, the goal is always the same: gain unauthorized access by posing as someone else. This category includes all phishing variants, such as *spear phishing*, *whaling*, *smishing*, *vishing*, *BEC*, and *consent phishing* — all united by their intent to compromise digital identity.

Phishing

What It Is

A type of online scam whereby attackers pose as trustworthy entities to trick users into revealing sensitive information such as passwords, account numbers, or Social Security numbers.

Why it Works

Phishing often mimics real emails from banks, streaming services, or tech providers. Victims click without thinking because the message looks familiar or urgent.

Tips to Protect Yourself

- Think before you open emails or click email links — examine URLs and sender addresses
- Use anti-phishing browser tools and spam filters
- Avoid logging in from links in emails
- Use physical security keys for logins instead of passwords

Spear Phishing

What It Is

A personalized scam email pretending to be from someone you trust — such as your supervisor or coworker — trying to trick you into clicking a link, sharing sensitive info, or transferring money.

Why it Works

It looks legit. The attacker researched you, your company, or your role.

Tips to Protect Yourself

Follow all protocols for “standard” phishing. In addition, always verify unusual requests with a phone call or other method. Don’t act on urgency alone.

Whaling

What It Is

A targeted phishing attack that targets high-ranking executives (the “big fish”) like CEOs, CFOs, or other decision-makers in a company.

Why it Works

Whaling emails often appear extremely professional and personalized. The stakes are higher because attackers aim for access to sensitive corporate systems, financial accounts, or trade secrets. Victims may act quickly due to authority, urgency, or the appearance of a legitimate business transaction.

Tips to Protect Yourself

- Verify wire transfer or sensitive requests through a second channel (e.g., a phone call)
- Become educated about scams that target executives and their red flags
- Use advanced email filtering and email authentication
- Deploy physical security keys for executive access points

Smishing (SMS Phishing)

What It Is

A phishing scam via text message. The message might claim to be from your bank, a delivery service, or even HR — with a link that leads to a fake login page.

Why it Works

Text messages feel more personal and urgent, and often people don’t scrutinize short links on mobile devices.

Tips to Protect Yourself

Scrutinize each text before reacting, and don’t click links in texts from unknown senders.

Vishing

Vishing (Voice Phishing)

What It Is

Vishing attackers use phone calls — often spoofing caller IDs — to trick individuals into giving up personal information such as passwords, account numbers, or Social Security numbers.

Why it Works

The human voice creates a false sense of legitimacy and urgency. Scammers often impersonate bank reps, tech support, government agencies, or even family members. The emotional tone and fast-paced nature of the call make it harder for targets to think critically or verify the caller's identity.

Tips for Protecting Yourself

- Never provide sensitive information over the phone unless you initiated the call to a verified number
- Hang up and call back using the official contact info from the company's website or official documents
- Use voicemail screening and call-blocking apps to limit exposure to robocalls or spoofed numbers

Business Email Compromise

Business Email Compromise (BEC)

What It Is

Attackers impersonate company executives or vendors over email, often requesting invoice payments, wire transfers, or confidential info.

Why it Works

It looks real — the email may come from a compromised account or closely spoofed domain. It often uses urgent language to bypass usual approval steps.

Tips for Protecting Yourself

Verify payment or information requests by phone or in person. Educate your team on signs of spoofing.

Consent Phishing

Consent Phishing

What It Is

A phishing scam that tricks you into granting permissions to a malicious app — like access to your email, contacts, or files — without stealing your password.

Why it Works

It looks like a legitimate request from Microsoft, Google, or a cloud provider, and the permissions seem harmless.

Tips for Protecting Yourself

Only grant permissions to known apps. Review what access an app is requesting.

Credential Stuffing

What It Is

A cyberattack where hackers take usernames and passwords from old data breaches and try them on other websites — hoping you reused the same login.

Why it Works

People reuse passwords across accounts, which makes them easy targets.

Tips for Protecting Yourself

Use unique passwords across accounts, enable multi-factor authentication (MFA), and avoid relying on passwords at all.

Password Spraying

What It Is

Hackers try common passwords (such as “123456” or “Spring2024”) across thousands of accounts, instead of targeting just one user.

Why it Works

Attackers avoid lockouts by using common passwords at a low rate across many usernames.

Tips for Protecting Yourself

Use long, unique passwords — or the best solution is switching to passwordless authentication.

Man-in-the-Middle (MitM)

What It Is

A hacker secretly intercepts the communication between you and a website, app, or device — often over public Wi-Fi.

Why it Works

It tricks you into thinking you're connected securely, when in fact your data is being monitored or altered.

Tips for Protecting Yourself

Avoid logging into sensitive accounts over public Wi-Fi, such as at coffee shops and airports. Use encrypted connections and device-based multifactor authentication.

Session Hijacking

Session Hijacking

What It Is

A hacker gains control of your active computer session — such as staying logged into your email, apps, or cloud accounts — without needing your login credentials.

Why it Works

If you're already authenticated, the attacker can piggyback off your open session. This can happen after phishing, malware, or insecure public Wi-Fi.

Tips for Protecting Yourself

Log out fully after use, use multifactor authentication, and avoid using public networks for sensitive work.

SIM Swapping

What It Is

A scammer convinces your mobile carrier to switch your phone number to a new SIM card — one they control.

Why it Works

Once the scammer has your number, they can receive your texts, reset passwords, and bypass text-based two-factor authentication.

Tips for Protecting Yourself

Use authenticator apps or physical security keys instead of SMS codes.

Account Takeover (ATO)

What It Is

An attacker gains full access to your account and locks you out — often through password reuse, credential stuffing, or SIM swapping.

Why it Works

The attacker often has your login credentials from another breach and may bypass weak authentication setups.

Tips for Protecting Yourself

Avoid password reuse and don’t rely on text-message codes. Use passkeys or physical security keys.

Replay Attack

What It Is

A replay attack involves an attacker intercepting legitimate data transmissions (like a login token or credentials) and reusing them to gain unauthorized access to a system or network at a later time.

Why it Works

Many systems don't verify whether a login session or token has already been used. If session data isn't encrypted or time-sensitive, an attacker can "replay" the transmission and fool the system into granting access.

Tips for Protecting Yourself

- Use time-stamped or single-use tokens that expire quickly
- Implement multifactor authentication to ensure intercepted data alone isn't enough
- Enable session expiration and anomaly detection in system security settings

Social Engineering

Social engineering is all about manipulating human behavior.

Instead of hacking systems, these attacks hack *people* — exploiting trust, urgency, fear, or curiosity. Whether it's scanning a malicious QR code or responding to a message from a fake executive, these scams rely on psychological manipulation to gain physical or digital access.

Pretexting

What It Is

An attacker invents a convincing scenario (a “pretext”) to get you to share sensitive information or grant access.

Why it Works

Attackers use emotion, urgency, or authority to persuade you, based on people’s propensity to be helpful or to obey authority.

Tips for Protecting Yourself

Stay skeptical of unfamiliar requests. When in doubt, verify the identity and purpose using another channel.

Baiting

What It Is

A social engineering attack that uses a tempting offer — like free downloads, movie files, or USB drives — to trick users into installing malware.

Why it Works

Baiting plays on curiosity and desire. Whether it's a "free gift card" or a "life changing app download," users often take the bait without realizing the danger.

Tips for Protecting Yourself

- Never plug unknown USB devices into your computer
- Avoid downloading free files from sketchy sources
- Use endpoint protection software
- Ensure your access points prompt for secure authentication

Quishing (QR Code Phishing)

What It Is

An attack using a QR code — typically on a poster, in an email, or even a fake sign in a public place — that leads you to a malicious website designed to steal your credentials.

Why it Works

QR codes are trusted by default and hard to verify at a glance.

Tips for Protecting Yourself

Only scan codes from trusted sources. Never log in to sensitive accounts through an untrusted QR code redirect.

Fake Online Stores

What It Is

Fake online stores are fraudulent websites designed to look like legitimate retailers. They lure shoppers with deals on popular or hard-to-find items, only to steal payment information or deliver counterfeit or no goods at all.

Why it Works

The appeal of low prices and urgency (“limited stock” or “flash sale” or “act now; almost gone”) leads people to trust appearances over verification. These stores often clone real brands or use social media ads to drive traffic quickly before being reported.

Tips for Protecting Yourself

- Stick to well-known retailers or verify unfamiliar stores through independent reviews and the Better Business Bureau before buying
- Look for proper SSL encryption (https://) and beware of oddly spelled URLs or poor grammar
- Avoid deals that seem “too good to be true”

Impersonation

(Non-AI) Impersonation Scam

What It Is

In a traditional impersonation scam, a criminal pretends to be someone you trust — like a boss, coworker, family member, or service provider — to trick you into transferring money, sharing sensitive information, or granting access.

Why it Works

Attackers exploit authority and urgency. A simple, believable request from someone "you know" (e.g., “Can you wire this money ASAP?”) can override your skepticism — especially when it’s crafted with real details obtained through public sources or prior research.

Tips for Protecting Yourself

- Always verify unusual or high-stakes requests through a second channel (e.g., call or text the person directly)
- Train staff and family members to spot red flags like urgency, secrecy, or unexpected changes in payment methods
- Implement strict internal protocols for financial transactions

Malware-Driven Attacks

Malware scams involve malicious software secretly installed on a device — often after clicking a link, downloading a file, or visiting a compromised website.

Once active, malware can steal data, spy on activity, or even lock users out entirely (*ransomware*). The attacker may use a *trojan horse* program disguised as something useful or set up a *drive-by download* that infects a user without any clicks.

Keylogging

Keylogging

What It Is

Malicious software (or hardware) that secretly records every keystroke you type — including usernames, passwords, and messages.

Why it Works

The user doesn't know it's happening. Keystrokes are captured silently and sent to the attacker.

Tips for Protecting Yourself

Use secure workstations, avoid installing unknown apps, and enable passwordless login where possible.

Ransomware

What It Is

Ransomware is a type of malicious software that locks, encrypts, or threatens to leak your data unless you pay a ransom to the attacker — often in cryptocurrency.

Why it Works

It causes immediate disruption and fear. Individuals and businesses may feel they have no choice but to pay, especially if backups are unavailable or critical operations are halted. Some attackers double-extort by threatening to publish sensitive files.

Tips for Protecting Yourself

- Back up your files regularly and store backups offline or in secure cloud storage
- Keep software and operating systems updated to patch vulnerabilities
- Use strong anti-malware and avoid clicking unknown links or attachments

Watering Hole Attack

Watering Hole Attack

What It Is

A watering hole attack infects a legitimate, high-traffic website that is frequently visited by a specific group (like employees of a company or industry). When users visit the site, they're unknowingly infected with malware.

Why it Works

It targets victims indirectly by compromising trusted digital "watering holes." Attackers research where their targets go online and infect those sites, relying on trust and routine to bypass skepticism.

Tips for Protecting Yourself

- Ensure software — including browsers and plug-ins — is updated with the latest security patches
- Use a secure web gateway and endpoint protection to detect malicious site activity
- Monitor high-value employee activity for suspicious behavior or downloads.

Drive-by Download

What It Is

A cyberattack where malicious code is automatically downloaded onto your device without your consent — just by visiting a compromised website.

Why it Works

Victims don't have to click anything to be impacted — simply loading the wrong page can be enough. These exploits often take advantage of browser or plugin vulnerabilities.

Tips for Protecting Yourself

- Keep browsers and plugins up to date
- Use ad blockers and antivirus software
- Avoid suspicious websites

Trojan Horse / Spyware

What It Is

Malware disguised as a legitimate file or program. Once installed, it can steal information, record activity (spyware), or open backdoors for attackers.

Why it Works

Trojans often appear as free apps or tools, convincing users to install them voluntarily. Spyware runs in the background, unnoticed — tracking every move.

Tips for Protecting Yourself

- Only download software from verified sources
- Run antivirus and malware detection tools regularly
- Enforce user permission controls

Emerging AI-Enabled Attacks

These cutting-edge scams are harder to spot — and require updated tools and awareness to defend against them.

With AI tools now widely available, scammers are leveraging generative AI to automate, personalize, and amplify attacks. AI can write highly convincing phishing emails, mimic a person's writing style, or generate fake voices and faces.

Deepfake Impersonation

What It Is

The use of AI-generated voice or video to convincingly mimic someone — often a company executive or authority figure — to trick people into taking harmful actions.

Why it Works

The impersonation sounds or looks real, especially over video calls or voicemail. It plays on urgency, authority, and fear of questioning a superior.

Tips for Protecting Yourself

Always verify sensitive requests with an alternate method, especially those involving money, passwords, or access.

AI-Generated Phishing Email

AI-Generated Phishing Email

What It Is

Phishing emails written by AI to sound more convincing, natural, and personalized — making them harder to detect than traditional phishing.

Why it Works

AI tools eliminate poor grammar and awkward phrasing, making fake emails seem legitimate. They may mimic a co-worker's tone or include specific personal details.

Tips for Protecting Yourself

- Provide regular phishing awareness training to staff
- Use email filters with AI detection capabilities
- Adopt passwordless, phishing-resistant login options such as FIDO2 physical security keys

THE LAYPERSON'S GUIDE TO

Security Scams Cheat Sheet

Quick Reference Guide

Scam	Description
CREDENTIAL & IDENTITY ATTACKS	
Phishing	A deceptive message tricks you into revealing credentials by impersonating a trusted source
Spear Phishing	A targeted phishing attack personalized with specific details about the victim to gain trust and access
Whaling	A spear phishing scam that targets high-level executives by mimicking urgent business requests
Smishing	A phishing attempt delivered via SMS or text message, often urging quick action
Vishing	A voice call impersonation scam used to extract personal or financial information
Business Email Compromise	An attacker poses as a company executive or vendor to trick employees into sending money or data
Consent Phishing	Users are tricked into granting malicious apps permission to access sensitive data without realizing it
Credential Stuffing	Stolen usernames/passwords from one breach used to access accounts where users reused credentials
Password Spraying	Attackers try common passwords across many accounts without triggering lockouts
Man-in-the-Middle	A hidden attacker intercepts communications between two parties to steal or alter data
Session Hijacking	An attacker takes control of a user's active session to impersonate them online
SIM Swapping	Attacker tricks mobile carriers into transferring your cell number to their device to intercept calls / texts
Account Takeover	A scammer gains control of your account and uses it for fraud, identity theft, or spam
Replay Attacks	An attacker intercepts and reuses valid data transmissions, like authentication tokens, to gain access
SOCIAL ENGINEERING ATTACKS	
Pretexting	Attackers create a fabricated scenario, such as a bank rep, to manipulate you into sharing private data
Baiting	A tempting offer, such as a free download or USB drive, is used to lure victims into installing malware
Quishing	A phishing tactic that uses malicious QR codes to trick users into visiting harmful websites
Fake Online Stores	Fraudulent e-commerce sites steal money or data by pretending to sell real products
Impersonation Scams	A scammer pretends to be someone you know or trust to gain access, money, or information
MALWARE-DRIVEN ATTACKS	
Keylogging	Malicious software secretly records your keystrokes to steal login credentials and sensitive data
Ransomware	Malicious software locks or encrypts your files and demands payment to restore access
Watering Hole Attacks	Hackers infect a trusted website likely to be visited by their target audience
Drive-by Download	Simply visiting a compromised website silently triggers a malware download without your knowledge
Trojan Horse / Spyware	Malware disguised as a legitimate program that secretly spies on you or damages your system
EMERGING AI-ENABLED ATTACKS	
Deepfake Impersonation	AI-generated video or audio mimics real people to spread misinformation or trick targets
AI-Generated Phishing Email	Attackers use AI to craft highly believable and personalized phishing emails at scale

KSI-2100: Your Frontline Defender

Most scams in this Guide start the same way: via password misuse, human error, or unattended access. For this reason, the security industry — and KSI — are moving toward phishing-resistant, presence-based, hardware-backed authentication.

The KS-2100 series keyboard is designed specifically to help prevent many of the scams outlined in this Guide. Our keyboard is a robust desktop security tool that can help prevent catastrophic security breaches with features that include:

- Type A & C physical security key ports that support FIDO2, passkeys, and physical tokens
- An integrated RFID/NFC reader that supports contactless smartcards and mobile access
- PresenceLock™ human presence detection for auto logoff to prevent unauthorized access

The KSI-2100 keyboard is ideal for shared workstations and zero trust environments where the protection of sensitive data is critical.

Superior Protection for

Financial Services

Manufacturing

Healthcare

Higher Education

Reach out for a demo or evaluation unit.

We have a desktop security solution in a form factor to fit your needs, whether it's integrated fingerprint biometrics, RFID, NFC, or human presence detection.

* **Disclaimer:** While we've included practical tips to raise awareness about scams and help you stay safer, this guide isn't meant to replace professional cybersecurity advice and is for educational purposes only. Use it as a helpful reference, not a guarantee.

14494 Wicks Boulevard
San Leandro, CA 94577
(510) 562-5000
info@ksikeyboards.com

youtube.com/user/ksikeyboards
x.com/ksikeyboards
linkedin/company/ksi-keyboards
ksikeyboards.com