

Malware and the Borrowed Face

Phishing tricks you into typing your password yourself. This article covers the other two doors into your computer and your accounts: **malware** — software that does the stealing for the criminal — and **impersonation**, where the scam arrives wearing a face you trust: a tech company, a government agency, or a family member's own voice.

Malware: the burglar you install yourself

Malware is simply a program working for a criminal. Once running on your computer it can record every keystroke including passwords, read your saved browser logins, watch your screen, or encrypt your files — decades of genealogy research included — and demand payment for their return. Modern versions are silent; an infected computer usually looks perfectly normal.

Here is the important part: malware almost never breaks in — it is invited. It arrives disguised as something you're persuaded to open or a step you're persuaded to perform. Which means the defense is not technical skill. It is recognizing the disguises below.

EXHIBIT A**The attachment wearing a paper mask****TRAINING EXAMPLE — THIS IS A FAKE EMAIL, ANNOTATED**

From: Records Fulfillment <no-reply@doc-delivery-center.net¹>

To: you@example.com

Your requested document is ready: Harris County probate index, 1897–1912

The archival document you requested is attached. This file will be deleted from our servers in 48 hours.²



Probate_Index_1897_scan.pdf.exe³

If the document does not open, choose "Run anyway" when Windows asks — this is normal for archival viewers.⁴

- 1 You didn't request anything.** The lure is tailored — genealogists get "archival records," others get invoices or shipping notices. An attachment you weren't expecting is hostile until proven otherwise, no matter how well it guesses your interests. Verify with the sender by a channel you already had, or delete it.
- 2 A countdown on curiosity.** "Deleted in 48 hours" exists to make you open it before you think — the same clock trick every scam relies on, aimed at your research instincts instead of your fear.
- 3 The double extension is the whole crime.** The name says PDF; the real ending — the part after the last dot — is .exe, a program. The moment it runs, the burglar is inside. Endings that mean "this is a program, not a document": .exe, .scr, .bat, .cmd, .js, .msi — and .zip containers holding any of them.
- 4 It coaches you past the guard.** "Choose Run anyway" is the tell that turns suspicion into certainty: Windows' warning is the last defense, and the email is pre-arguing against it. A real document never needs permission to "run."

The document version of "Run anyway": the Enable Content button

Some malicious attachments really are Word or Excel files — with a hostile program hidden inside as a "macro." Office opens them safely in Protected View, showing a yellow bar with an **"Enable Content"** or **"Enable Editing"** button. A document that *instructs you to click that button* to view it is the paper mask again: no genuine record needs macros to be read. Close it instead.

EXHIBIT B**The fake "prove you're human" test — on a real website****TRAINING EXAMPLE — THIS IS A FAKE WEBPAGE, ANNOTATED**

Address bar: countyrecordslookup-example.org/search-results

Verification required to view this page

☒ I'm not a robot

To complete verification:

1. Press **Windows key + R**
2. Press **Ctrl + V** (the code is already copied)
3. Press **Enter** ¹

- 1 No real verification ever asks you to press keys on your keyboard.** Windows-key+R opens your computer's "Run" box; the page has already placed a hidden command on your clipboard; Enter executes it — you have just installed the burglar personally, on a website that may be a perfectly legitimate site that was hacked. This trick (security researchers call it "ClickFix") is one of the fastest-growing infections of 2026. The rule is absolute: any webpage, popup, or "support agent" that tells you to press Windows+R, paste, and hit Enter is attacking you — leave the site.

TRAINING EXAMPLE — THIS IS A FAKE BROWSER POPUP, ANNOTATED

⚠ WINDOWS DEFENDER SECURITY CENTER — CRITICAL ALERT ⚠

Your computer has been LOCKED. Trojan spyware "Zeus2026" detected. Your banking passwords and photos are being transmitted. ¹

Do not shut down or restart your computer — this will cause total data loss. ²

Call Microsoft Support immediately: +1 (866) 555-0170 (toll-free) ³

(In the real version, a siren plays through the speakers and the page fills the whole screen)

- 1 Real security warnings don't scream.** Windows Defender's genuine alerts are quiet notifications from the system itself, in the corner of the screen. A flashing full-page alarm with sound is a *web page* — an advertisement dressed as your computer. Nothing has been detected; nothing is being transmitted.
- 2 It forbids the one action that defeats it.** "Don't restart" is there because closing the browser or restarting ends the whole theater. That is exactly what to do: close the browser (press and hold the power button if the screen truly won't respond). Nothing will be lost.
- 3 Microsoft does not put phone numbers in warnings** — and never calls you, either. The number connects to a call center that will ask for remote access to "clean" your machine, then bill you hundreds, or worse (see Exhibit D). No legitimate alert from Windows or Apple ever includes a phone number.

EXHIBIT D**The invoice that wants a phone call****TRAINING EXAMPLE — THIS IS A FAKE EMAIL, ANNOTATED**

From: SecureShield Billing <receipts.dept.4471@gmail.com¹>

To: you@example.com

Receipt: your SecureShield Total Protection renewal — \$389.99

Thank you for renewing SecureShield Total Protection. Your card on file has been charged \$389.99 for a 3-year plan. This charge will appear on your statement within 24 hours.

Did not authorize this renewal? Our refund desk can reverse the charge today:

Call +1 (877) 555-0102 — available 24/7²

Order #SS-2026-77841 · SecureShield Inc.

- 1 A software company billing from a free Gmail address.** Provenance again — no real company issues receipts from a personal mailbox. Note there's no dangerous link or attachment anywhere: that's deliberate, because the trap is the phone number, and phone numbers sail past every email filter.
- 2 The fake charge exists to make YOU place the call.** No charge has happened — check your statement and you'll find nothing. But if you call, a friendly "refund agent" will ask to connect to your computer with remote-access software to "process the reversal," then show you a fake mistyped refund and pressure you to return the difference — by bank transfer or gift cards. Once that software is installed, they have everything. If you suspect any charge, call the number on your card statement, never one from a message.

EXHIBIT E**The call from your bank's "fraud department"****TRAINING EXAMPLE — A FAKE PHONE CALL, TRANSCRIBED AND ANNOTATED**

Caller ID shows: FIRST NATIONAL BANK — the same name and number printed on your card ¹

Voice: "Ma'am, this is Marcus with First National fraud prevention. We've flagged a \$2,400 charge at a Best Buy in Miami — did you authorize that? ... I didn't think so. We can block it, but I need to verify you first. I'm sending a six-digit code to your phone right now — read it back to me and I'll cancel the charge. ²"

Later in the call: "Your checking account itself is compromised, ma'am. We're issuing you a new account — I'll help you move your balance to the secure holding account right now. It has to be done by wire while we're on the line, before the suspects drain it. ³ And please don't visit the branch or discuss this — two tellers are under internal investigation. ⁴"

- 1 Caller ID is not identification.** The name and number on the screen are typed in by the caller, like the return address on an envelope — spoofing them is trivial. A call that *looks* like your bank carries exactly zero proof it is. The fix costs one minute: hang up and dial the number on the back of your card yourself. A real fraud department expects and respects this.
- 2 Reading back the code hands over your account.** The scammer is on your bank's real website at that moment, resetting your password — the texted code is the bank trying to stop *him*. This is the same never-share-a-code rule from the phishing guide, in spoken form: no bank employee will ever ask you to read one aloud.
- 3 There is no such thing as a "safe account."** Banks secure a compromised account by freezing it and reissuing cards — never by having you wire the balance somewhere while you're kept on the phone. "Move your money to protect it" ends the conversation by itself, whoever appears to be calling — bank, FBI, Social Security, or Medicare.
- 4 Secrecy and urgency, the eternal pair.** The invented teller investigation exists to stop you walking into a branch — where a real human would end the scam in one sentence. Any caller who forbids you to verify is telling you exactly what verification would reveal.

The government costume, and the family costume

Government: Social Security, Medicare, the IRS, and police do not call or email about suspended benefits, warrants, or "safe accounts" — they write letters, and no agency on earth takes payment in gift cards, wire transfers, or cryptocurrency. Any such demand identifies itself as fraud in the same sentence.

Family: AI tools can now clone a relative's voice from seconds of video, well enough to carry a panicked phone call. One defense defeats the most advanced version of this scam with a 1960s technology: **a family code word**. Agree on one phrase; any urgent call about money gets asked for it, then a call-back on the number you've always had. A cloned voice cannot answer, and a real grandchild won't mind.

Why scammers choose the payment method for you

Every scam steers you toward a specific way to pay — always the kind that cannot be pulled back. Knowing the ladder is a defense in itself:

How they ask you to pay	Can it be reversed?	What it means when requested
Gift card codes	Never — spent in minutes, untraceable	Always a scam. No company, court, or agency accepts them.
Wire transfer	Almost never — gone on arrival	A demand to wire money to a stranger, "safe account," or fee office is a scam.
Cryptocurrency / Bitcoin ATM	Never — designed to be irreversible	No legitimate business or agency directs you to a crypto ATM. Ever.
Zelle / instant payment apps	Rarely — treated like handing over cash	For friends and family you know in person — never for strangers, "refunds," or fees.
Check / bank transfer	Sometimes, if reported fast	Speed of reporting decides everything — call the bank the same hour.
Credit card	Usually — strong dispute rights by law	The safest way to pay anyone you haven't fully verified.

The rule that falls out of the table: the harder a payment is to reverse, the harder a scammer will push you toward it. Anyone who refuses a credit card but demands gift cards, wire, or crypto has answered your question about who they are.

Five things no legitimate caller, company, or agency will EVER ask

- ❶ To install remote-access software (AnyDesk, TeamViewer, UltraViewer) so they can "help" or "refund" you
- ❷ To read them a security code that was texted or emailed to you
- ❸ To pay anything with gift cards, cryptocurrency, or a wire to a "safe account"
- ❹ To press Windows+R and paste a command, or to click "Run anyway"
- ❺ To keep the call secret from your family or your bank

Each of these ends the conversation by itself. You don't need to figure out the rest of the story — hang up, close the page, tell someone.

Hardening your computer and accounts: twelve recommendations

Roughly in order of protection per minute of effort. The first five close the doors malware actually uses; the rest limit the damage if something gets through.

- ➊ **Let your computer update itself.** Turn on automatic updates for Windows or macOS and your browser, and restart when asked. Most malware exploits holes that were patched months earlier — updating is free immunity.
- ➋ **Trust the antivirus you already own.** Windows includes Microsoft Defender; it is genuinely good and already on. What you must know is how real warnings look: quiet notifications from the system itself. Any full-screen browser alarm with a siren and a phone number is the theater from Exhibit C — close the browser, don't call.
- ➌ **Never open unexpected attachments, and read the last extension.** If the part after the final dot is .exe, .scr, .bat, .cmd, .js, or .msi — or a .zip you weren't expecting — delete it. When a real-looking document surprises you, confirm with the sender by phone before opening.
- ➍ **Install software only from the maker's own site or the official app store.** Never from a download button in an ad, an email, or a popup — and never because a webpage says your Flash, font, or "archival viewer" is out of date.
- ➎ **Adopt the Windows+R rule.** No website or caller ever has a legitimate reason to have you open the Run box and paste anything. Teach it to friends — this one is new enough that most people have never been warned.
- ➏ **Back up what you can't replace — automatically.** Your family tree files, scanned documents, and photos should live in at least two places: the computer and either a cloud backup or an external drive that isn't left plugged in. Ransomware can only destroy copies it can reach; a current backup turns catastrophe into inconvenience.
- ➐ **Use a standard account for daily use if you share a computer.** Malware inherits the power of the account that runs it; an administrator account hands it the whole machine.
- ➑ **Keep two-step verification on email and banking:** even if a keylogger steals a password, the thief still hits a locked second door.

- 9 **Freeze your credit at all three bureaus** — Equifax, Experian, and TransUnion. It's free, takes twenty minutes, and makes stolen personal information nearly useless for opening accounts in your name. Unfreeze temporarily whenever you actually need credit.
- 10 **Review bank and card statements monthly for small strangers.** Thieves test cards with tiny charges before large ones; a \$2.17 charge you don't recognize deserves a phone call.
- 11 **Establish the family code word this week** — and while you're at it, agree that no family emergency is ever handled by gift card. Rehearsing the response once, out loud, is what makes it available under pressure.
- 12 **If a machine is compromised, get help and report it.** Disconnect it from the internet, run a full Defender scan, change passwords from a different device (email first), call your bank if money is exposed, and report at ic3.gov. Local library and senior-center tech help is real and free — using it is the smart move, not the embarrassing one.

Forged attachments, fake verification tests, screaming popups, and borrowed faces — different costumes, one skeleton: **urgency, secrecy, and an unverifiable claim of authority.** Genealogists have been unmasking that skeleton in the archives for years. The inbox is just a newer archive.

About this article: prepared by Family Sentinel — a Texas-based service that monitors your email for indications of compromise and malicious or destructive messages, and provides comprehensive safety checks and live support for internet and email security concerns. Learn more at **FamilySentinel.org**. The example emails, webpage, popup, and phone call shown are fictional training composites; the companies and domains do not exist.

Reprint permission: clubs, churches, libraries, and community groups are welcome to photocopy and distribute this guide unmodified, free of charge.