

The Counterfeit Login Page

Phishing is not hacking. Nobody breaks into your account — you are invited to walk into a counterfeit one. The scammer builds a pixel-perfect copy of a login page you trust, sends you a reason to visit it, and you type your password into their form yourself. Here is exactly how the invitation looks, and the habits that make it useless.

Phishing succeeds because the fake is genuinely good. The email copies the bank's real logo and typefaces; the counterfeit login page is often an exact clone of the real one. What the scammer cannot copy is **the address it is served from** — a web address is registered property, like a deed. That single fact is the foundation of every defense on this page: you cannot reliably judge a page by how it looks, but you can always judge it by where it lives.

#1

phishing is the most-reported cybercrime to the FBI, year after year — by a wide margin

Hours

a stolen email password is typically used within hours — first to reset your other accounts

0

legitimate reasons anyone will ever ask you to read them a security code from your phone

Source: FBI Internet Crime Complaint Center (IC3) annual reports.

How to read a web address

Scammers rely on people reading addresses left to right and stopping at the first familiar word. Browsers work the other way: **the owner of the page is the last name-and-ending immediately before the first single slash.** Everything to the left of it is decoration the scammer controls.

<https://www.chase.com/security/alerts>

✓ Owned by **chase.com** — the genuine bank. Words after the slash are just pages on their site.

<https://chase.com.verify-alerts83.com/login>

✗ Owned by **verify-alerts83.com** — a stranger. "chase.com." at the front is bait; it is merely a nickname the true owner prepended.

<https://secure-chasebank-login.com>

X A brand name woven into a longer domain is still a different domain. Chase owns chase.com, not every address containing the word "chase."

<https://chase.com.co/login>

X One extra syllable changes the owner. ".com.co" is not ".com" — and neither is "chase-secure.net", "chasse.com", or "cnase.com". Lookalike spellings are registered by the thousand; when the stakes are money, **type the address yourself or use your bookmark** rather than proofreading a stranger's.

Genealogists already do this instinctively: a will filed in the wrong county is suspect no matter how authentic the handwriting looks. **Jurisdiction first, contents second.**

The padlock myth

The padlock icon beside a web address means the connection is *encrypted* — nothing more. It says your conversation with the site is private; it says nothing about who the site is. Scam sites buy the same padlock certificates legitimate ones do, for free, in minutes. **A padlock on a counterfeit page just means you are being robbed over a secure connection.** Judge the address, not the icon.

EXHIBIT A**The security alert that steals the account it warns about****TRAINING EXAMPLE — THIS IS A FAKE EMAIL, ANNOTATED**

From: First National Security Team <alerts@firstnational-secure-id.com¹>

To: you@example.com

Unusual sign-in detected — your account will be locked in 12 hours²

Dear Customer,

We detected a sign-in attempt from Kyiv, Ukraine at 3:47 AM. If this was not you, your account access will be restricted within 12 hours unless you verify your identity.

Verify My Identity Now³

Link destination: [https://firstnational.com.id-check-4417.net/secure/login⁴](https://firstnational.com.id-check-4417.net/secure/login)

For faster service, have ready: your online banking password, the card number on file, and the one-time code we will text you during verification.⁵

First National Bank · Member FDIC

- 1 The sender's domain is not the bank's.** "firstnational-secure-id.com" is a domain anyone could register this morning for a few dollars. Your bank writes from the same domain you log in at — nothing else.
- 2 Fear plus a countdown.** A frightening event (a foreign sign-in) paired with a deadline is the phishing formula. It is designed to make checking the details feel like wasted time you can't afford.
- 3 The button is the trap.** The entire email exists to make this one click feel urgent and reasonable. Whatever a security email claims, the safe response is identical: close it, and log in by typing the bank's address yourself or using your bookmark. If something is genuinely wrong, the message will be waiting inside your account.
- 4 Read the destination right-to-left.** The true owner is id-check-4417.net — "firstnational.com." at the front is the nickname trick from the anatomy box above. This one habit defeats the majority of all phishing.
- 5 It rehearses you for total compromise.** Password, card number, and the texted code — that last item is the six-digit code that exists precisely to stop thieves who already have your password. Anyone who asks you to relay a texted code, by any channel, for any reason, is stealing the account. No bank employee will ever ask.

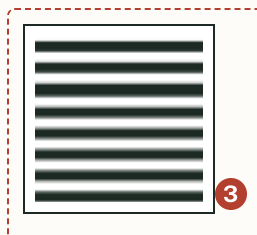
EXHIBIT B**The QR code — a link you cannot read****TRAINING EXAMPLE — THIS IS A FAKE EMAIL, ANNOTATED**

From: North Texas Toll Services <tollservices@payment-portal-txn.info¹>

To: you@example.com

Unpaid toll balance: \$6.84 — avoid a \$48.50 late penalty

Our records show an unpaid toll of \$6.84 from your recent travel on the Dallas North Tollway. To avoid a late penalty of \$48.50 and a hold on your vehicle registration, scan the code below with your phone camera to pay now²:



(This example code is deliberately unreadable — never scan codes from suspicious mail)

Payment must be received within 24 hours to avoid referral to collections and DMV registration hold.⁴

- 1 The toll authority writing from a stranger's domain.** Same provenance check as always — and note the costume: a name shaped like your local toll agency. Fake toll-fee messages are among the most common phishing lures in Texas right now, by text and by email.
- 2 The QR code exists to blind you.** With a written link you can hover or press-and-hold to preview the destination. A QR code removes that ability — you can't read one, so the right-to-left habit is defeated. That is exactly why scammers switched to them. Treat any QR code in an unexpected email as a link you're forbidden to inspect — and therefore refuse.
- 3 Scanning moves the attack to your phone** — a smaller screen where the address bar is harder to read, and where you're less likely to have protection. If you ever do owe a toll, look up the agency's site yourself and check your account there.
- 4 A small debt, a large penalty, a short clock.** \$6.84 is deliberately trivial — cheap enough to pay without thinking. The real target is the card number you type on the payment page, not the seven dollars.

EXHIBIT C The DNA match that wants your password — phishing aimed at genealogists

TRAINING EXAMPLE — THIS IS A FAKE EMAIL, ANNOTATED

From: LineageHub DNA <matches@lineagehub-notifications.net¹>

To: you@example.com

New DNA match: Close Family — First Cousin (shared cM: 912)²

You have a new DNA relative!

A member matching **912 centimorgans** with your kit has joined LineageHub — our system estimates a **first cousin or half-sibling** relationship. They have sent you a message and attached a photograph.

Sign in to view your match »³

Link destination: [https://lineagehub.com.member-login-portal.cc/auth⁴](https://lineagehub.com.member-login-portal.cc/auth)

Match messages are held for 72 hours before being archived.⁵

LineageHub DNA · Member Notifications

- 1 A notification domain that isn't the service's own.** Genealogy platforms send mail from the same domain you log in at. A separate "-notifications.net" address is a stranger's property wearing the brand.
- 2 The lure is engineered for this audience.** A close-family match is the one email a genealogist cannot ignore — a possible half-sibling rewrites the tree. The specific centimorgan number is set dressing; scammers copy the real notification's wording precisely because it works.
- 3 The button leads to a counterfeit login page** — a perfect copy of the sign-in screen. Type your password there and the thief now controls your account: your tree, your DNA data, your messages to other members, and — because most people reuse passwords — often much more.
- 4 Right-to-left, as always:** the owner is member-login-portal.cc, not the genealogy service. The habit works on every lure, including the ones aimed straight at your hobby.
- 5 The gentle 72-hour clock.** Softer than a threat, but the same mechanism: act before you think. If the match is real, it will be waiting in your account when you log in through your own bookmark — matches are never "archived" away from you.

Why genealogists are targeted by name: your surname interests, your society memberships, and often your email address are publicly posted on forums, trees, and

member directories. That is not a reason to hide — it is a reason to expect tailored bait and judge every message by its address, not its subject line.

EXHIBIT D**The shared document from a name you know****TRAINING EXAMPLE — THIS IS A FAKE EMAIL, ANNOTATED**

From: CloudDocs Sharing <share-notify@clouddocs-fileservice.com¹>

To: you@example.com

Barbara Hartley shared "Hartley Family — Estate Documents (Final).docx" with you²

Barbara Hartley has shared a document with you:

 **Hartley Family — Estate Documents (Final).docx**

Open Document³

Link destination: [https://docs-viewer-secure.net/open?file=884213³](https://docs-viewer-secure.net/open?file=884213)

You will be asked to confirm your email address and password to verify you are the intended recipient.⁴

CloudDocs · This link expires in 24 hours

- 1 A generic "cloud sharing" service you've never used.** Real sharing notices come from the platform the sender actually uses — and even those are worth suspicion, because this lure is also sent through hacked accounts of people you genuinely know.
- 2 A real name, harvested.** "Barbara" may be a friend whose address book was stolen, or a name lifted from the same public family tree you posted. Estate and inheritance titles are chosen because family curiosity overrides caution. If Barbara really shared a file, a phone call to Barbara settles it in one minute.
- 3 The "document" is a login page.** The link opens a counterfeit email sign-in — "verify yourself to view." No legitimate document requires your email password to read. The moment a shared file asks you to log in to your *email*, close the page.
- 4 Your email password is the crown jewels.** Whoever holds it can press "Forgot password?" at your bank, your brokerage, and your genealogy sites — and reset them all. That is why this lure asks for the email login rather than anything about the document itself.

What makes phishing fail: ten habits

None of these require technical skill. Each one removes a tool the scammer depends on.

- ❶ **Never log in through a link that came to you.** Email, text, or QR — it doesn't matter how real it looks. Reach your bank, email, and medical portals only through your own bookmarks or by typing the address. This single habit defeats nearly all credential phishing by itself.
- ❷ **Read every address right-to-left.** The owner is the final name-and-ending before the first single slash. If it isn't exactly the company's real domain, close the page.
- ❸ **Preview before you click, always.** Hover with a mouse; press-and-hold on a phone or tablet. If the preview doesn't match the text of the link, that mismatch is your answer.
- ❹ **Use a password manager, and let it do the typing.** Beyond convenience, it has a hidden superpower: it fills your password only on the exact site that saved it. A perfect counterfeit page leaves it silent — and that silence is a phishing alarm no human eye can match.
- ❺ **Give every important account its own password.** Phishing one password should cost you one account, not your email, bank, and genealogy subscriptions at once. The manager from #4 makes this effortless.
- ❻ **Turn on two-step verification for email and banking** — an authenticator app or, better, a passkey, rather than texted codes where offered. It turns a stolen password from a catastrophe into a nuisance.
- ❼ **Never read or type a security code for anyone.** The six-digit codes texted to your phone exist to stop thieves who already have your password. Banks, Medicare, Microsoft, your grandson's "IT department" — nobody legitimate will ever ask you to share one.
- ❽ **Refuse QR codes in unexpected messages, on parking meters, and on flyers.** A QR code is a link you cannot read. If the destination matters, find it yourself by typing the organization's address.
- ❾ **Protect the email account above everything.** Whoever controls your email can reset your other passwords with "Forgot password?" It deserves your strongest password and two-step verification first.

- 10 When in doubt, verify out-of-band.** Close the message and contact the organization through a number or address you already had — the back of your card, a saved bookmark, an old statement. Legitimate organizations survive the ten minutes this takes. Scams do not.

If you typed your password into a page you now doubt

Change that password immediately from a device you trust — and anywhere else the same password is used, starting with your email. Turn on two-step verification if it wasn't on. If card or bank details were entered, call the number on the back of the card the same hour; banks can often stop or reverse fraud that is reported fast. Then report the site at **ic3.gov**. Speed matters far more than embarrassment — this is a crime that catches careful people daily.

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 shown are fictional training composites; the senders 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.