



How to Tell What's Real Online

Smarter everyday digital habits



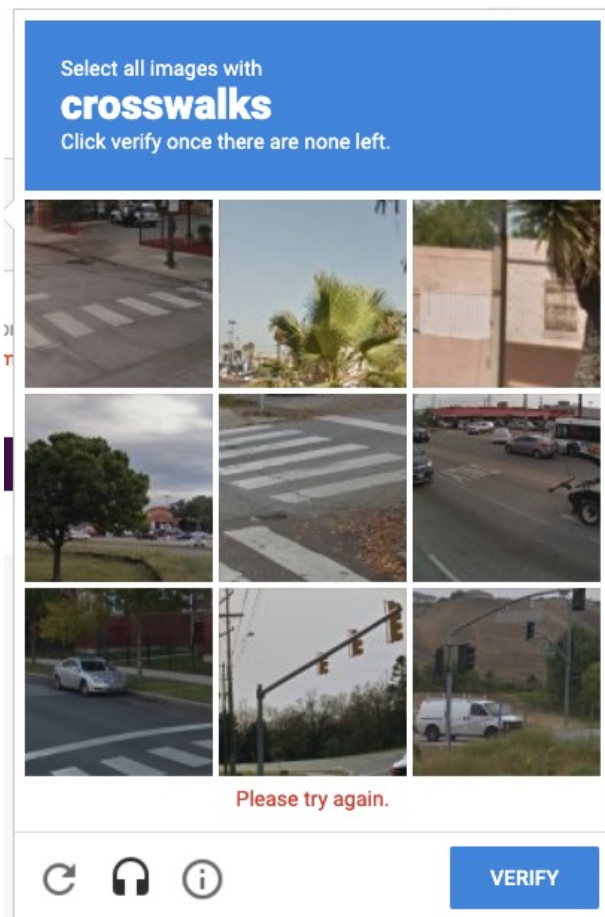
Deception is the fundamental engine of modern cybercrime. Instead of breaking into systems, many criminals trick people into giving them access. That is why everyday digital habits are essential to help you recognize when someone is trying to deceive you to get into your accounts.

When a CAPTCHA Isn't Just a CAPTCHA

One way scammers can deceive individuals is through CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) prompts, which can appear on websites. These are the familiar tests that ask you to select images containing crosswalks, cars, bridges, or traffic lights. (See example to the right)

CAPTCHAs are not automatically suspicious, but context matters. If one appears on a site you visit regularly, such as a trusted e-commerce website, it may be entirely normal. If it appears on an unfamiliar site, contains misspellings, or is followed by unusual instructions, proceed with caution.

That same lesson extends beyond CAPTCHAs. Appearances alone are not enough to establish trust online.



How to Spot a Suspicious Website

A polished logo, familiar color scheme, or professional-looking page does not necessarily mean a site is legitimate. These websites are designed to look convincing. Before entering personal information, check the web address carefully to make sure there are no unusual domains, misspellings, or subtle variations. Using a saved bookmark, a trusted app, or manually typing the website address can help reduce the risk of landing on a fraudulent site.

Staying Safe on Public Wi-Fi Networks

Public Wi-Fi networks can also be an area where deception occurs. Connecting to public Wi-Fi is not inherently dangerous, but it is less predictable than a trusted home network. For sensitive activities such as banking or accessing investment accounts, it is generally safer to use your home network, cellular connection, or a personal hotspot.

When accessing a financial account, using the institution's official app can be a better choice than searching for its website in a browser, provided the app comes from an official app store and is kept up to date. Downloading the official app from a trusted source can reduce the chance of landing on a fake website. For additional protection, a VPN can add another layer of defense on public networks, although it is not a cure-all against online threats.

Even when you're using trusted networks and applications, it is important to verify the information you rely on.

Verifying Phone Numbers and Contact Information Online

It is important to be careful with phone numbers found online. Search results can be manipulated, and AI tools can sometimes produce incorrect answers with confidence. If you need to contact a bank, custodian, government agency, or technology company, use a number from a trusted source. Trusted sources to find this information include your statement, the back of your payment card, the official app, or the organization's verified website.

The common thread in each of these examples is simple: verify before you trust.

General Tips for Internet Safety

Individuals and families should follow a simple rule of thumb when interacting online: if something is urgent, financial, or unusual, verify it through a separate channel before acting. That might mean calling back using a known number, logging directly into the account, or confirming the request with someone you trust.

Having this level of digital awareness requires discipline, but in a digital environment where deception is often the first tool of cybercriminals, slowing down and verifying information remains one of the most effective ways to protect yourself.