U.S. ARMY
CYBER COMMAND

www.arcyber.army.mil | Follow @arcyber

Fraudulent Websites

According to Internet security experts, thousands of fraudulent websites are built every day to try to lure visitors into giving away personal and financial information, buy products that don't exist, or download malware that disrupts devices and data.

Scammers can easily create phony websites that look very real. They may even include phony reviews and a fake address -- or even the actual street address of an unsuspecting business -- to snare victims. These are often linked to phishing scams, such as crooks sending an email saying your bank account has been compromised and you need to change your password. Clicking a link in the email takes you to the fake but real-looking site, where any information you enter is nabbed by the scammer.

WHAT ARE SOME EXAMPLES OF FAKE SITES?

- Online stores that advertise incredible deals but steal payment information or trick visitors into buying fraudulent or nonexistent products.
- Pages that look like the login pages to services or popular websites.
- Sites with malicious pop-ups that can download malware to steal sensitive information.
- Health care or health insurance sites that swipe medical data by asking users to verify account information.
- Package delivery websites that ask users to verify their personal information or trick them into giving up their credit card numbers.
- Airfare booking sites that steal personal information such as passport or credit card numbers or sell fake tickets.

WHAT ARE SOME WAYS TO IDENTIFY FAKE SITES?

- Take a good look at the domain name to ensure it matches the official website. Fake sites often use domain names similar to official URLs or that may even contain the official URL.
- Look for a closed padlock or tune icon in the site's address bar that indicates a site has a valid security certificate to block hackers. But scammers can also use certificates to fool visitors into beliving fake sites are real, so it's a good idea to click on the padlock to learn more about the certificate. Information such as registered company name, country of origin, province or state, and locality are signs that the site uses greater security to make it harder to fake.
- Use a website checker that can verify secure sites. There are free online tools such as Google Transparency Report that checks billions of URLs daily for unsafe sites.
- Check to see how long the site has been active. Fake sites normally don't last long. Tools such as Whois and Wayback Machine can provide details such as the owner's organization name, country of registration, and age of the domain.

- Watch for poor spelling and grammar; bad site design such as pixelated or low-quality images or logos; difficult navigation; and missing sections or business details such as contact information, phone numbers and physical address. Be wary if the only way to contact the business is with a generic form. Street addresses can be checked with an online mapping program or the U.S. Postal Service website, and regulatory government authorities where the business is supposedly located can verify whether it exists.
- Trust your instincts and beware of deals that seem too good to be true.
- Look for reviews on the site and other locations, such as the Better Business Bureau, that warn of fraudulent site practices. But be aware that reviews can be phony, too. You can often spot fakes if there are many similar-sounding reviews; if all the reviewers are new to the platform; if the reviews have too few or too many details; or if the reviews are all unusually positive.
- Check shipping, return and other policies. Scam sites normally won't provide return information, as well as other items found on legitimate sites such as basic legal information, terms and conditions, and privacy and data collection policies.
- Check payment options. Fake websites often ask for payment using non-reversible or non-traceable methods such as gift cards, bank transfers, cryptocurrencies, or payment apps, while legitimate sites always offer safer and more traditional options such as credit and debit card payment.
- Beware of "trust signals". Studies show that most customers are more likely to shop on sites that display items that are supposed indications of their worthiness, such as industry awards, certifications or security logos. Contact the issuing organizations to verify that these are real.

HOW CAN I REPORT FAKE SITES?

- Report fake websites, emails, malware, and other Internet scams to the FBI's Internet Crime Complaint Center at https://www.ic3.gov/
  If you need to report an international scam, report it to the International Consumer Protection and Enforcement Network at https://www.econsumer.gov/en/Home/FileAComplainit/1#crnt
  Frauds and scams can also be reported to the Federal Trade Commission at https://reportfraud.ftc.gov/
- You can also report phishing, fake or unsafe websites to Google at https://safebrowsing.google.com/safebrowsing/report_phish/ and to Microsoft at https://www.microsoft.com/en-us/wdsi/support/report-unsafe-site/