41 Ways

to Uncover the Truth of Someone's Digital Identity

CODE SIGNING
STORE

41 Ways to Uncover the Truth of Someone's Digital Identity

There are plenty of ways you can determine whether a website, person, or organization is legitimate. Here are a few helpful tips to make you more informed.

While protecting your own digital identity online is very important, it's also important to know how to determine whether someone else's online identity is real. Here's how to check...

How to Tell If a Website Is Legitimate

The internet has billions of websites where you can search for the latest apps, games, videos, and buy the latest tech. But not all of those websites are real. Many are fake and are created to trick you into giving them your personal or financial info, or to get you to make a bogus purchase. Thankfully, you don't have to fall for their tricks. Here's how to tell if a site is real or fake.

1

Double-check the URL. This is #1 on our list because it's so important. If you accidentally type in the wrong web address, you could find yourself on a look-alike scam site! For example, make sure you're on **amazon.com** and not **amzon.com**. Look for added or missing letters, numbers, or even missing/extra periods where there shouldn't be one.

2

Check the certificate details. Whenever you visit any website, check to ensure that the site's owned by a real company. Look for a padlock in the web address bar, click on it, and see if it displays any company info in the certificate details.

3

Review the site content. Does the design feel off in some way? Are the images stretched or pixelated or does the site have content that doesn't make sense? Are there a lot of ads or popups? All of these could be signs of a fake website.

4

Research the company on Google. Search for the company name to see what info is available and how recent that information is. (Is all the information new, or does it have a track record dating back several years?)

- Check out company, product & service reviews on Google, Yelp, and other related sites.
- Review scam reports and star ratings. Do they have a lot of 1-star reviews?
- Look up the company's information on **whitepages.com**. You can use this information to compare it to other search results.

5

Use the BBB. The Better Business Bureau is a great resource for reading about the legitimacy and reputation of a company.

6

Perform a Google street search. Yeah, you can totally do that! See if that address has a real building with a business logo on it. If the address shows an open field or another non-identifying location, run the other way!

7

Check the state's business directory. This is easier than it sounds. Check our your state's business directory for more information about the company.

8

Check the site's ICANN data. Using the **icann.com** website, you can look up a domain's registered company information and see related address and phone number information. You can then compare this to the company's official **whitepages.com** listing to see if it matches.

9

Check the domain on URLvoid.com. This site is a great way to check a website's reputation, registration information, location info, and to see if the domain is on any blacklists.

How to Tell If a Social Media Profile Is Real

Social media is everywhere, and its number of users grows by the day. HubSpot reports that there are 4.2 billion social media users globally. But how can you tell whether someone's social media profile is legit? Here are a few things to look for when evaluating the social profile of a person or organization.

10

See if their profile is verified. On Twitter and Instagram, you can see if profiles of well-known people are verified because they'll have a checkmark ✓ that informs you. This is mainly limited to celebrities and influencers.

11

Reach out to the person through another channel. If someone you know in RL appears to reach out on a new profile, make sure it's really them. Do this by calling them on the phone or asking them about it face to face.

12

Look out for duplicate profiles. Cybercriminals like creating fake profiles to gain access to your personal info or to join your (or your friends') social networks. Having this connection makes their fake profiles seem more believable.

13

Check the age of the profile. See when profile was created. Has it been around for a while (months or years), or was it recently created? How recently were images and info added to it? Were they added all at once or over time?

14

Review their network connections. If someone tries to connect with you, see if you know anyone else in their network.

15

See if their photos are real. Perform a reverse image search on Google to see if a picture is real or if it's been used on other people's profiles, websites, or stock image sites.

16

Ask them a few hard questions. If messaging with the person, ask them something only the real person would know.

17

Create a fake scenario & gauge their response. Ask a question or make a comment about a fake teacher at your school and see what they say. If you ask them about an example Mr. Smith covered in your math class, and there is no Mr. Smith, then you'll know the person is lying.

18

See if they have endorsements on LinkedIn. If you receive any connection requests on LinkedIn, see if they have any endorsements from real people and if they have any connections to the organizations they claim to work at (or worked at previously).

How to Tell If an Email Is Real

Email is a primary mode of communication, especially when you start working. People of all ages fall for phishing emails and other email-related scams every day. So, what can you do to prevent yourself from falling for them as well? Here are a few key things to look for when checking emails you receive to see if they're legitimate.

19 **Inspect the email address.** Does the display name match the email address? Look carefully at the email domain (the info after the "@" symbol) and see if it's legitimate. Are there any added or missing letters or numbers?

20 **Read the email header information.** This is a more in-depth step, but it can provide you with additional information about the sender.

21 **Look for spelling errors and typos.** Legitimate businesses take the time to carefully review communications. See If there are any obvious misspellings of words or weird grammatical mistakes.

22 **Read the language.** Is the email written in a way that creates a sense of urgency, fear, or dread? Does it make you feel like you have to do something RIGHT NOW or something bad will happen? That may be an indication of a phishing or malicious email.

23 **Watch out for unsolicited attachments.** Does the email contain Office files, PDFs, images, or other attachments you didn't request? If so, it may be malicious software that's disguised to look like a legitimate file. Never open attachments from unsolicited messages or unknown senders.

24 **Does the email make sense?** Ask yourself if the message or what's being requested in it makes sense. Is the message out of the blue? Are you really expecting a package? Do you have a subscription to that account? Think critically and check for other red flags before responding to an email or clicking on any links.

25 **Check embedded links.** Don't click on links in emails without checking where they lead! By check, we mean hover your mouse over any links and buttons and see the URL that pops up. Does it match the website it claims to lead to? If not, don't click.

26

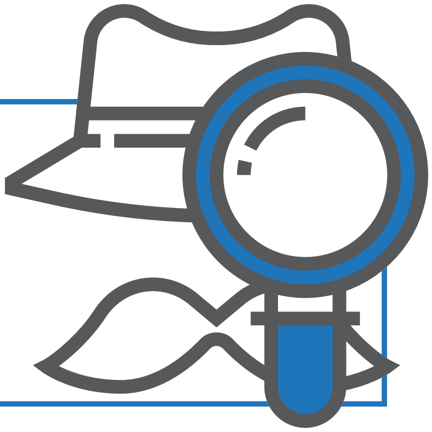
Use a URL expander. Ever get emails that contain shortened URLs like bit.ly or ow.ly? Never click on unknown links like this. Instead, you can copy-and-paste the shortened URL into a URL expander tool and see what the full URL looks like.

27

Trust your gut. If something feels off or just doesn't feel right, trust your instinct. Show the email to a parent or another adult.

How to Tell If an App Is Legitimate

Software applications are integral to technology. If you're like most teens, you use software applications on your computer and smartphone on a daily basis to play games, edit photos, or work on projects. But how can you tell if an app is real and not a phony?



28

Download apps from legitimate stores. Google Play and Apple review apps before adding them to their app store lists. Never download apps or software from third-party apps stores and file-sharing sites like Torrent.

29

Check the publisher info. Before downloading an app, be sure to check the publisher's information. (We've already covered some of those methods previously in the website section.) Ask yourself: Is this a legitimate and reputable company?

30

Look for verified publisher info. Whenever you download software onto your computer, look for verified publisher information.

31

Read their reviews. Does the app have a lot of 5-star reviews? How about 1-star reviews? See how recent the reviews are and if they appear to have been added all around the same time.

32

Review app permissions. Look at the permissions app is requesting. If an app is requesting a lot of unnecessary permissions, it may indicate that someone is using the app to gain access to your personal data or spy on you.

33

Read reviews from other sources. Look up company's name followed by terms like "review," "rating" or "scam" and see what pops up.

How to Tell If a Text or Phone Call Is Legitimate

This is where things get tricky. There's a trick called spoofing that some cybercriminals like to use to send texts or make phone calls from phone numbers that don't belong to them. So, there are some things you can do to try to identity if a call or text is legit.

34

Ignore unknown callers. Robocallers and cybercriminals will call from many different — and often spoofed — phone numbers. If you receive a call from an unknown number, let it go to voicemail. If it's real and important, they'll leave a message so you can call them back. Otherwise, let it go.

35

Look out for common scams. Phone scammers often use a few specific rouses (although they do use others as well). Some of the most common include pretending to be:

a. The IRS,
b. Police or other law enforcement,
c. Medicare/Medicaid,
d. Tech support (Apple, Microsoft, Amazon, etc.)
e. An unspecified "car warranty" company,
f. Free stuff (money, giveaways, vacations, gift cards, etc.) and
g. A job or college recruiter

36

Are they pressuring you? Ask yourself if you feel like the caller is trying to pressure you to do something or to give up personal information immediately. This is a commonly used scam tactic.

37

Ask the caller to provide specific information. If someone calls up claiming to be from a company you have an account with or applied for a job at, ask which one. Watch out for language like "I'm so-and-so calling about your job application." Ask them, from what company? Ask yourself if you applied to that company.

38

Have them provide info you can verify. If you think a call may be legitimate but want to make sure, have them share information that you can verify. Never provide personal information to someone over the phone unless you initiated the contact.

39

Look on a company's official website for a telephone number. If someone calls claiming to be from your bank, for example, hang up and call them back using an official phone number. (Never provide personal info to someone who reaches out to you unexpectedly!)

40

Run a Google search. See if the phone number is linked to any scam or spam reports. Also, see if the phone number is linked to a lot of different names or businesses. This is a good indication that the number isn't legitimate.

41

Check the WhitePages. Use **whitepages.com** to look up the phone number that's calling you and see if it matches any legitimate companies or people.

Knowing how to spot a person or organization's digital identity is essential to your safety on the internet. Digital identity helps you know whether you should engage with someone online or over the phone. It also helps you determine if an online business is safe to buy products or download apps from.