Club Bytes Vol 4, May 2022

Brought to you by the Lake Gaston Computer Club

Word of the Month - Lurking

On the internet, "lurking" is the act of being in an interactive community, like a group chat or a forum, but not directly participating or getting involved. Lurking is passive observation of a public conversation. People who do this on the internet are often called "lurkers." Read more. https://www.howtogeek.com/771896/what-is-lurking-online/

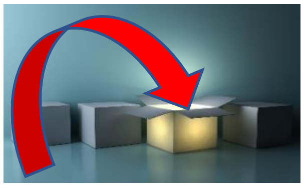
TidBits - Anonymous

Lake Gaston Computer Club Gus Best Scholarship

If you wish to donate for the scholarship, make a check payable to LGCC Gus Best Scholarship. All donations are tax deductible as we are a 501-C3 organization. You should mail your donations to Lake Gaston Computer Club, P.O Box 1533, Littleton, NC 27850.

List of Committees are on the Lake Gaston Computer Club website. Click on the Link below.
https://www.lakegastoncc.org/contact.html

Member Suggestion Box - **Bright Idea>** **president@lakegastoncc.org**



If you have a suggestion for the computer club, please send it to president@lakegastoncc.org Examples: classes, presentations at monthly meetings, SIGs, newsletter articles.

From the Repair Shop:

Something Not Working?

Have No Fear, We Are Here!

Interested in sharing your computer and software talents with other Club members? Please call the Repair Shop at 252-586-9919 if you can join us on Mondays.

- **The number one issue for the Shop is forgotten passwords**. Use a password manager or keep a written list in a secure location. The Shop is unable to recover lost or forgotten passwords!

- **Did you replace your aging computer over the holidays or perhaps have an old one in a closet, basement or garage taking up valuable storage space?** Consider donating it to the computer club. The repair shop refurbishes old computers for worthy causes in our community and for sale to club members to raise operating funds. What can't be refurbished will be recycled in a responsible way. We don't refurbish or donate printers.
  The **Repair Shop** in Littleton will only accept donations of all types of computers, tablets, and smartphones on Mondays from 8:30am to 2:30pm.

- The current Windows 10 version is 21H2 (OS Build 19044. 1682).
- The current Windows 11 version is 21H2 (OS Build 22000. 652).

- The current Mac operating system is Monterey iOS 15.3.1.
- The current iPad and iPhone operating system is iOS 15.4.1.

- To check your Windows version, type the word Winver in the bottom left search box (or magnifying glass) then click Winver in the choices list. If you need to update, type the word Update in the bottom left search box (or magnifying glass) then click

Check for Updates in the choices list. On the next screen, click Check for Updates; do this even if it says you are up to date. Keep clicking Check for Updates as long as the updates keep coming in.

- Do not download the optional updates; they are not needed unless you have a specific driver problem.

- Since Windows 10 will be supported by Microsoft until October 2025, there is no need to update from Windows 10 to Windows 11 at this time. Give Microsoft time to work out the bugs and problems with their new operating system.

How to Spot a Fraudulent Website MARSHALL GUNNELL

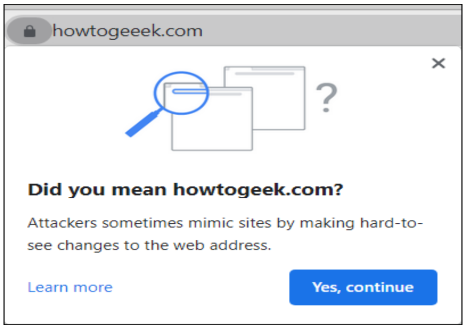
The internet is home to roughly 1.7 billion websites. Unfortunately, many of these websites live only to scam you out of your personal data or money. Here are a few signs to look out for to spot a fraudulent website.

1. Double-Check the URL Name

The first thing you should do before visiting a site is ensure that the domain name is the one you intend to visit. Fraudsters create fake sites masquerading as an official entity, usually in the form of an organization you would recognize, such as Amazon, PayPal, or Wal-Mart. Sometimes the difference between the real site's name and the fraudulent site's name is almost unnoticeable. For example, the cybercriminal may build a site using *rnicrosoft.com* (note the "r" and "n" at the beginning of that address, which looks like an "m"), but you think you're visiting *microsoft.com*.

There are two basic ways the cybercriminal, or "threat actor," gets you to visit the fraudulent site. The first way is by a method known as "phishing." Phishing is a form of cyberattack that is delivered by email. The threat actor tries to entice you to click a link in the email that will then redirect you to a fraudulent copy of the real website.

Another way the threat actor may get you to visit the fraudulent site is by a method known as "typosquatting." Typosquatting uses common misspellings of domain names (for example, amazom.com) to trick users into visiting fraudulent websites. You think you entered the domain name correctly, but you're visiting a fraudulent copy of the genuine site. If you're lucky, your web browser will warn you.



howtogeeek.com

Did you mean howtogeek.com?

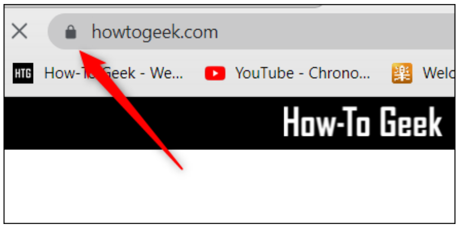
Attackers sometimes mimic sites by making hard-to-see changes to the web address.

Regardless of how you get to the site, once you log in to this fraudulent website, the threat actor will harvest your login credentials and other personal data, such as your credit card information, and then use those credentials themselves on the actual website or any other website where you're using the same login credentials.

The first and most basic method of spotting a fraudulent website is to make sure the domain name is the one you truly intend to visit.

2. Look For the Padlock, Then Look Harder

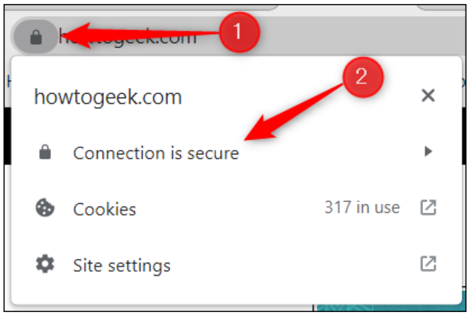
When you visit a website, look for the padlock to the left of the URL in the address bar. This padlock indicates that the site is secured with a TLS/SSL certificate, which encrypts data sent between the user and the website.



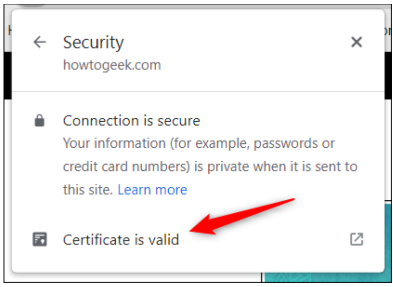
If the website hasn't been issued a TLS/SSL certificate, an exclamation mark (!) will appear to the left of the domain name in the address bar. If a site isn't TLS/SSL certified, any data you send is at risk of being intercepted.

The downside to this is that not all SSL certificates are authentic. These sites are usually caught quickly, but it's still best to look a little harder at the padlock just to be sure. Unfortunately, you can only dig deeper if you're browsing the web using a desktop.

First, click the padlock and then click "Connection is Secure" from the context menu.

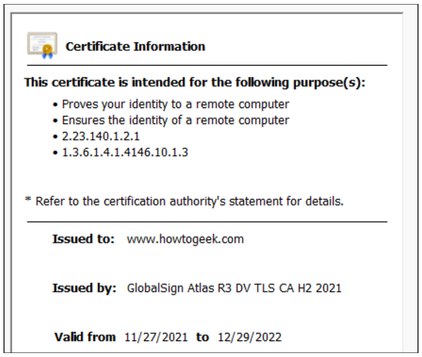


If the certificate is valid, then you'll see the "Certificate is Valid" text on the next menu. Go ahead and click that for more details.



Your information (for example, passwords or credit card numbers) is private when it is sent to this site. Learn more

A new window displaying the information about the certificate will appear. You can check which site the certificate was issued to, who it was issued by, and its expiration date.



Certificate Information

This certificate is intended for the following purpose(s):

- Proves your identity to a remote computer
- Ensures the identity of a remote computer
- 2.23.140.1.2.1
- 1.3.6.1.4.1.4146.10.1.3

* Refer to the certification authority's statement for details.

Issued to: www.howtogeek.com

Issued by: GlobalSign Atlas R3 DV TLS CA H2 2021

Valid from 11/27/2021 **to** 12/29/2022

While this won't always protect you from fraudsters, the padlock (and the certificate information) is a good indicator that you're visiting a legitimate site.

3. Check the Site's Privacy and Return Policies

Fraudulent websites generally don't go to the extent that genuine websites go to concerning privacy and return policies, if at all. For example, Amazon has a pretty thorough return policy and privacy policy that details everything the customer needs to know about each respective policy.

If a site has a poorly written return or privacy policy, that should raise some red flags. If a site doesn't have these policies stated on their website at all, avoid them at all costs, as the site is likely a scam site.

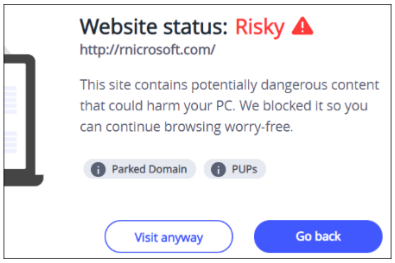
4. Check For Poor Spelling, Grammar, and UI

A spelling or grammar mistake is likely to happen now and again, even on the most authoritative of websites. However, most websites have teams of professionals creating these websites. If a website looks like it was created in a day by one person, is riddled with spelling and grammar errors, and has a questionable user interface (UI), there's a chance that you're visiting a dangerous website.

5. Use a Site Scanner

If you'd like to add another layer of protection between you and fraudulent websites (and also give you a heads up if you may be visiting one), then use a site scanner such as McAfee SiteAdvisor.

These tools crawl the web and test sites for spam and malware. If you visit a dangerous (or potentially dangerous) site that the program determines may contain dangerous content that could harm your PC, you'll be notified and asked to confirm you still want to proceed to the site when you try to visit.



Website status: Risky ⚠

http://rnicrosoft.com/

This site contains potentially dangerous content that could harm your PC. We blocked it so you can continue browsing worry-free.

While site scanners are helpful in spotting a potentially fraudulent website, not all fraudulent websites will be flagged. While you use them as an extra layer of protection, still be conscious of the sites you visit.

6. What to Do If You've Been Scammed

If you're a victim of an online scam, there are a few measures you can take to protect yourself (and potentially protect others). What you need to do next depends on what type of information you believe the scammer may have on you.

If you purchased something using your credit or debit card from the fraudulent site, the first thing you should do is **call your bank immediately** and report to them what happened. They'll freeze your accounts and cards so that the threat actor can no longer purchase anything with your details.

If you believe the threat actor may also have your personal information, such as your Social Security Number, date of birth, address, and so on, you'll want to freeze your credit so that the fraudster can't take out any loans or open any accounts in your name.

Once that's taken care of, file a report with your local police, notify the Internet Crime Complaint Center (IC3), your State Attorney General, and report the site to Google. You can bring your computer to the Repair shop, and they will help you scan for any harmful software which may have been placed on your computer. You may also need to change the username and password to your router.

Internet Connection Not Working? 10 Troubleshooting Tips

TIM BROOKES

https://www.howtogeek.com/721045/internet-not-working-10-tips-to-troubleshoot-a-connection/

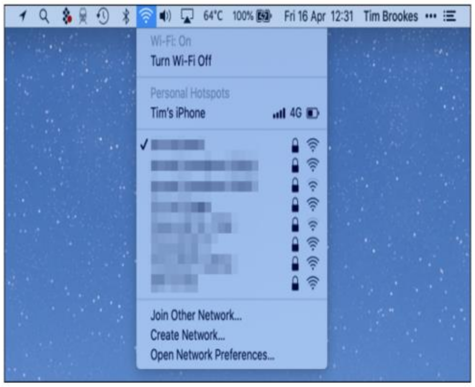
It's useful to have a checklist of things to try when your internet is not working. Sometimes you can fix the problem yourself, while other times, it's caused by a problem with your service provider. Here's how to pin down and fix the problem.

1. First, Check Whether Your Connection Is Down

Sometimes the problem isn't your internet connection at all. If you're trying to access a website that simply won't work, it might just be a problem with that web page. You can try performing a search or checking social media to see whether those services are working, or you can query the website in question with a service like downfor.io.

2.Test Your Local Connection

If you're still getting nothing, check the local connection between your device and your network hardware. A glance at the system tray on Windows or at the menu bar on a Mac will show whether you are connected via a wired or a wireless connection. On a smartphone, look for the Wi-Fi symbol or head to your device settings and attempt to connect from there.



If you're connected via Wi-Fi but the internet still isn't working, this points to a problem with your online connection. If you can't find your wireless network, this points to a problem with your network hardware.

3. Reset Your Wireless Connection

Occasionally, some devices seem to "forget" that they are meant to be connected via Wi-Fi. Using your wireless settings to set up the connection again might be all that it takes to get your local connection working again.

Your devices will remember login credentials and other information about your local connection. If this changes, your computer, or smartphone might be trying to connect with the wrong information. You can try to "forget" the wireless network using your device's wireless settings and reconnecting again.

(go back to the link at the beginning of the article for in depth info)

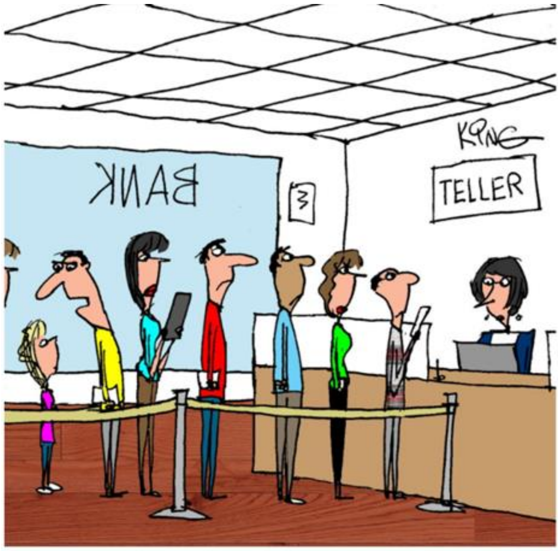
4. Using Ethernet? Check Your Cables
5. Try Restarting the Problem Device
6. Ensure That Network Hardware Is Working
7. Reboot Your Router
8. Check the Connection Status on Your Router/Modem
9. Try Another Device to Isolate the Issue
10. Try Changing Your DNS Servers

Remember: If you try another device and get similar results, it's likely that your internet connection is to blame. At this stage, it's a good idea to contact your service provider and report a fault. Be aware that some smartphones switch to cellular data when no local network connection is detected (although they should tell you about it), so you might want to turn off cellular data temporarily if you're testing this on a smartphone.

If the thought of spending time on the phone with your service provider sends shivers down your spine, consider switching to a better provider. Our preferred way to pick a provider is by searching for the fastest ISP in your area.

Keep your home Wi-Fi safe in 6 simple steps

Written by Dan Rafter for NortonLifeLock



*"Tell me about online banking again.
I'm not good at technology, but it's got to be
less stressful than this."*

How much do you rely on your home Wi-Fi? If you're like most people, you use it for online banking, for paying your credit card, for reserving hotel rooms, for chatting with friends and for watching movies.

That's a lot of activity. And in many cases, everything from laptops and phones to security systems, thermostats, and air conditioners are all connected to home Wi-Fi.

This is a benefit. But when not safeguarded, your home Wi-Fi network can be a playground for scammers, hackers, and other cybercriminals. A small vulnerability in your home Wi-Fi network can give a criminal access to almost all the devices that connect to that network. Hackers and scammers might be able to access your online bank accounts or credit card portals. They might be able to spy on those emails you send to your doctor. They might even flood your devices with malware and spyware.

Fortunately, you can secure your home Wi-Fi network with some simple steps and doing so can keep the cybercriminals at bay.

Here are some key tips to help secure your home Wi-Fi network against unauthorized access.

1. Change the default name of your home Wi-Fi

First, change the SSID (service set identifier), or name, of your home Wi-Fi network. Many manufactures give all their wireless routers a default SSID. In most cases it is the company's name. When a computer searches for and displays the wireless networks nearby, it lists each network that publicly broadcasts its SSID. This gives a hacker a better chance of breaking into your network. It is better to change the network's SSID to something that does not disclose any personal information, thereby throwing hackers off their mission.

2. Make your wireless network password unique and strong

Most wireless routers come pre-set with a default password. This default password is easy to guess by hackers, especially if they know the router manufacturer. When selecting a good **password** for your wireless network, make sure it contains at least 20 characters, including numbers, letters, and symbols. The more complicated your password, the more difficult it is for hackers to break into your network. Need help creating and remembering a strong password? Utilize Norton Password manager included in your subscription to help generate passwords strong enough to safeguard your personal information.

3. Enable network encryption

Almost all wireless routers come with an encryption feature. For most routers, though, it is turned off by default. Turning on your wireless router's encryption setting can help secure your network. Make sure you turn it on immediately after your broadband provider installs the router. Of the many types of encryptions available, the most recent and effective is "WPA2."

4. Turn off network name broadcasting

When using a wireless router at home, it is highly recommended that you disable network name broadcasting to the general public. When nearby users try to find a Wi-Fi network, their device will show a list of nearby networks from which they can choose. If you disable name broadcasting, though, your network won't show up, keeping your Wi-Fi connection invisible to those who don't know to look for it.

This feature is useful for businesses, libraries, hotels, and restaurants that want to offer wireless internet access to their customers, but it is unnecessary for a private wireless network, including your home Wi-Fi network.

5. Keep your router's software up to date

Sometimes a router's firmware, like any other software, contains flaws that can become major vulnerabilities unless they are quickly fixed by their manufacturers' firmware releases. Always install the latest software available for your router and download the latest security patches immediately. This will increase the odds that hackers won't be able to access your Wi-Fi network.

6. Use VPNs to access your network

A **virtual private network**, or VPN, creates an encrypted data tunnel that helps protect the data that you send and receive on Wi-Fi. Individuals can use VPNs, like Norton Secure VPN which is included as part of your Norton 360 subscription, as a method to secure and encrypt their communications. When you connect to a VPN, a VPN client is launched on your computer. When you log in with your credentials your computer exchanges keys with another server. Once both computers have verified each other as authentic, all your Internet communication is encrypted and hidden from outside prying.

Most of all, check what devices are connected to your home network and make sure they have Norton Security installed on every device to help protect against viruses and spyware.

Help secure your accounts with these strong password tips

Written by a NortonLifeLock employee

It's no secret that passwords have substantial monetary value to cybercriminals. The importance of using secure, unique passwords is growing as you entrust increasing amounts of personal information to organizations and businesses that can fall victim to data breaches and password leaks. Although there may be little you can do to prevent a large-scale data breach, you can take the precaution of making sure you craft strong usernames and passwords for your online accounts.

How to create a strong password

Follow these tips to help yourself craft unique, complex passwords.

1. Do not use personal information

Don't use your name or names of family members or pets in your passwords. Don't use numbers like your address, phone number, or birthdays, either. These can be publicly available, on forms you fill out or on social media profiles, and easily accessible to hackers.

2. Do not use real words

Password cracking tools are very effective at helping attackers guess your password. These programs can process every word in the dictionary, plus letter and number combinations, until a match is found. Steer clear of using real words from the dictionary or proper nouns or names.

Instead, use special characters. By combining uppercase and lowercase letters with numbers and special characters, such as "&" or "$," you can increase the complexity of your password and help decrease the chances of someone potentially hacking into your account.

3. Create longer passwords

The longer the password, the harder it may be to crack. Try for a minimum of 10 characters.

4. Modify easy-to-remember phrases

One tip is to think of a passphrase, like a line from a song, and then use the first letter from each word, substituting numbers for some of the letters. For example: “100 Bottles of Beer on the Wall” could become “10oBb0tW”.

5. **Don’t write them down**

Resist the temptation to hide passwords under your keyboard or to post them on your monitor. Stories about hackers getting passwords by rummaging through trash, also known as dumpster-diving, are absolutely real.

When you type your password in a public setting, make sure no one is watching or looking over your shoulder.

One way to store and remember passwords securely is to use a tool that keeps your list of usernames and passwords in encrypted form. Some of these tools, called password managers, will even help by automatically filling in the information for you on some websites.

6. **Change passwords on a regular basis**

Passwords for your online financial accounts should be changed every month or two. Computer login passwords should be changed at least once a quarter. Using the same password for longer periods could put your information at risk if a data breach occurs.

7. **Use different passwords on different accounts**

Don’t use the same password on more than one account. If a hacker cracks it, then all the information protected by that password on other accounts could also be compromised. Norton Password Manager to help create unique and strong passwords.

8. **Do not type passwords on devices or networks you do not control**

Never enter your password on another person’s computer. It could be stored without your knowledge.

When using your devices on public Wi-Fi, you should avoid visiting websites that require you to log in to your account, such as online banking or shopping. When you’re on an unsecured public network, your unencrypted data could be intercepted by a nearby hacker. To protect yourself from these threats, you should always use a virtual private network (VPN), like Norton Secure VPN, when on a public Wi-Fi connection.

9. **What is two-factor authentication, and how does it work?**

Two-factor authentication, or 2FA, is a method of verifying your identity that adds a second layer of security to your account password. Types of two-factor authentication can include any of the following:

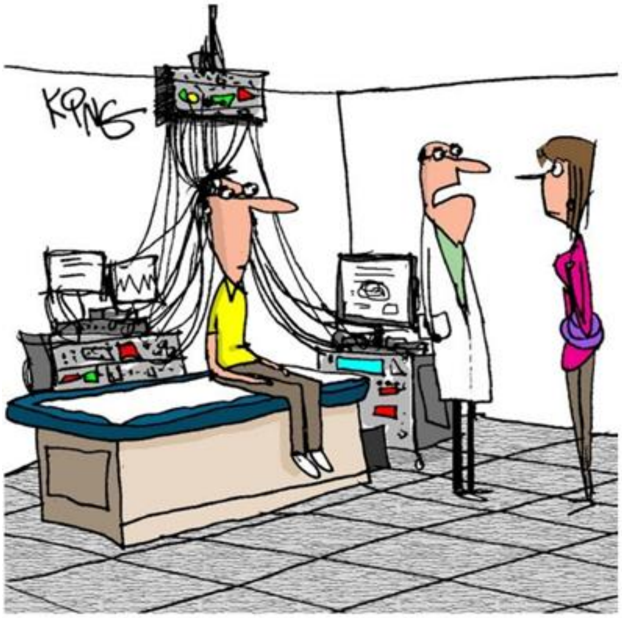
- Something you know: a PIN number, password, or pattern
- Something you have: an ATM or credit card, mobile phone, or security token
- Something you are: a biometric form of authentication, such as your fingerprint, your voice, or your face

10. Extra security for your passwords

With two-factor authentication (2FA), you get an extra layer of security that hackers may not be able to crack as easily, because the criminal needs more than just the username and password credentials. You may already be using 2FA without realizing it. Your ATM card is an example, combining your physical card and your PIN. Remember that nothing is 100% secure, and even 2FA can be vulnerable to hackers. If a cybercriminal gains access to the email account associated with your 2FA information, they could reset your password by selecting "Lost/Forgot password" on a given site's login page. This password recovery option could completely bypass 2FA and allow the hacker to create a new password, locking you out of your account. Be sure to monitor your email account for messages requesting password changes.

Look for a Password Manager plan that provides you with the tools you need to create, store, and manage your passwords, credit card information, and other credentials online - safe and in a secure vault.

- It should store and remember all your usernames, passwords and more so you don't have to
- Automatically fills in your usernames and passwords for you
- Let's you access usernames, passwords and other profile information from your Mac, PC, or mobile device
- Securely stores addresses and other important information to help fill in online forms for fast online checkout
- Warns you of suspicious sites while you surf and search the web on your mobile device



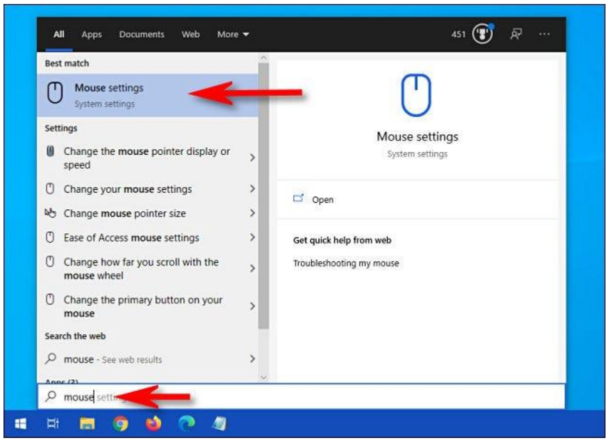
"It took some time, but we were able to locate the password he's been needing. Please tell him to write it down when he gets home."

How to Quickly Locate Your Mouse Pointer on Windows 10

By Benj Edwards, How-to Geek

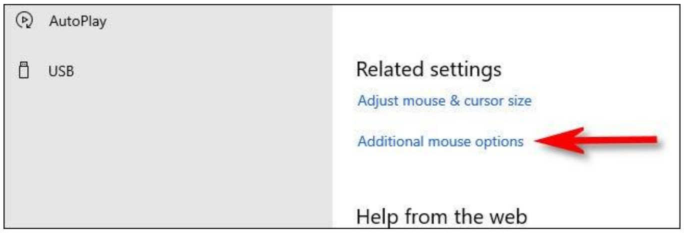
If you often lose your tiny Windows 10 mouse pointer in your football-field-resolution display, there's a way to quickly locate the wayward arrow by pressing the Ctrl key. Here's how to turn it on.

First, open the Start menu and type "mouse." Then click the "Mouse settings" shortcut that appears.



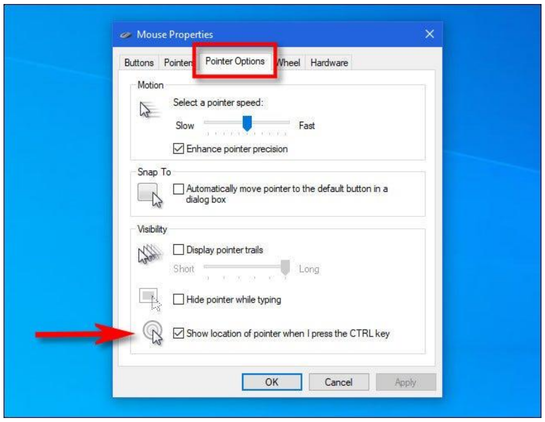
"My mouse is running from me. Apparently, he's tired of me slamming him down when I get frustrated with my computer. I even apologized."

In Mouse settings, locate the "Related settings" section and click the "Additional mouse options" link.



When the "Mouse Properties" window opens, click the "Pointer Options" tab, and place a checkmark beside "Show location of pointer when I press the CTRL key." Then click "OK."

Tip: If you lose your cursor often, you might want to consider turning on "Display pointer trails" in this window as well.



Select a pointer speed:

☑ Enhance pointer precision

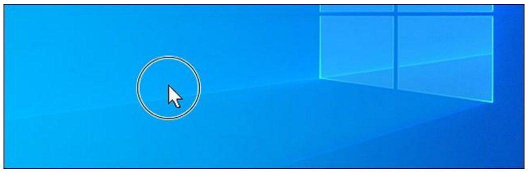
☐ Automatically move pointer to the default button in a dialog box

☐ Display pointer trails

☐ Hide pointer while typing

☑ Show location of pointer when I press the CTRL key

The “Mouse Properties” window will close. Exit settings as well. Now, any time you can’t find your mouse cursor on the screen, just press the Ctrl key. An animated shrinking circle will appear around the cursor.



Use it as many times as you’d like, and you’ll never lose your mouse cursor again. Happy computing!

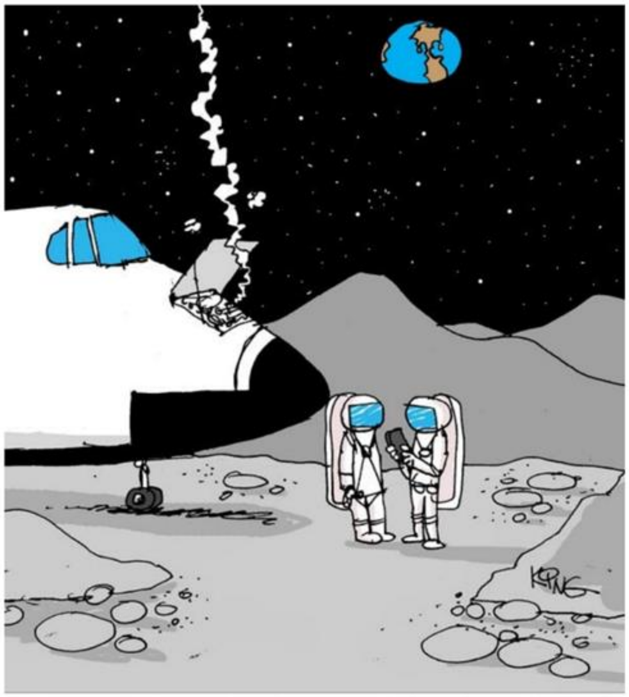
Just a Bit of Humor

"Yes, it is a gaming mouse, but that doesn't mean you can play catch with it."

"When they hired me, they asked if I would mind if I got my hands dirty. I thought it would be more adventurous than changing the ink in all the printers."

"Tell the delivery guy he was off about 100 feet again."

"Instead of coming from old money, I, unfortunately, come from old computers."



"I just called an Uber. The cost is $50 million, plus tip."

"Tech support said to run a full antivirus software scan. If that doesn't work, our second option is to panic and run."

"I tried using the garage code to get into the computer. I tried using the computer password to get into my phone. I tried using the phone password to get into the garage..."

"Apparently, you didn't learn your lesson when you tried cleaning your phone screen like that."

I am looking for member(s) with journalistic talents to help with the newsletter. If interested, please contact communications@lakegastoncc.org

Until next month