5 FACEBOOK SECURITY TIPS

If you've been using Facebook for a few years, then it's likely your account contains a lot of private information. Cybercriminals love seeing accounts with lots of information because they are often easy to breach.

While Facebook does have various privacy and security settings to keep your personal information safe, you still need to act as your own bodyguard to maintain total security. Your account password is the first and best security measure for keeping invaders at bay, so take this tip seriously. Make sure your password is at least 12-14 characters in length and contains no personal information. That type of information could very well be visible on your profile page, making your password much easier to guess.

Facebook makes it easy to see when your account has been logged into. Enabling login alerts allows you to see what device accessed your account and where it was accessed. In addition, enable two-factor authentication on your account, which Facebook calls "Login Approvals". This can be done by going to Settings, then Security and Login., and selecting Use two-factor authentication.

Continued on next page

5 FACEBOOK SECURITY TIPS *cont.*

You may either choose to get a notification on Facebook, through email, or sent via text message. The next time anyone logs in from an unrecognized device or browser, you'll be notified.

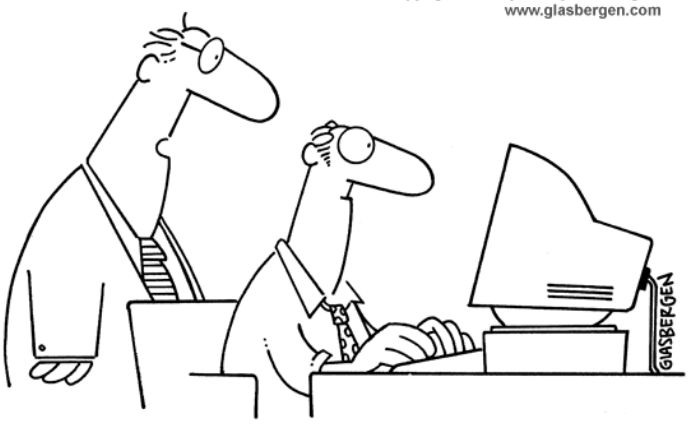
Be mindful that having an excessive friends list could leave you vulnerable. You should remove friends that are inactive or are not actually your friends in "real life". This can seem like an overwhelming task, especially if you have anywhere between 750 to 1,000 "friends" listed. However, it is a necessary security measure that all users should do regularly. There are tons of phony Facebook profiles out there. Clear out all unwanted friends, friends you don't know, and remain meticulous in the accepting future friend requests.

We all know that phishing scams are common in emails, but they can also be present in direct messages sent through Facebook. Keep an eye out for messages sent through Facebook Messenger that contain incorrect spelling or tell you to click on the provided link to visit other websites. Clicking on unknown links may compromise your account and allow hackers to post their own phishing scams on your Facebook wall without you knowing

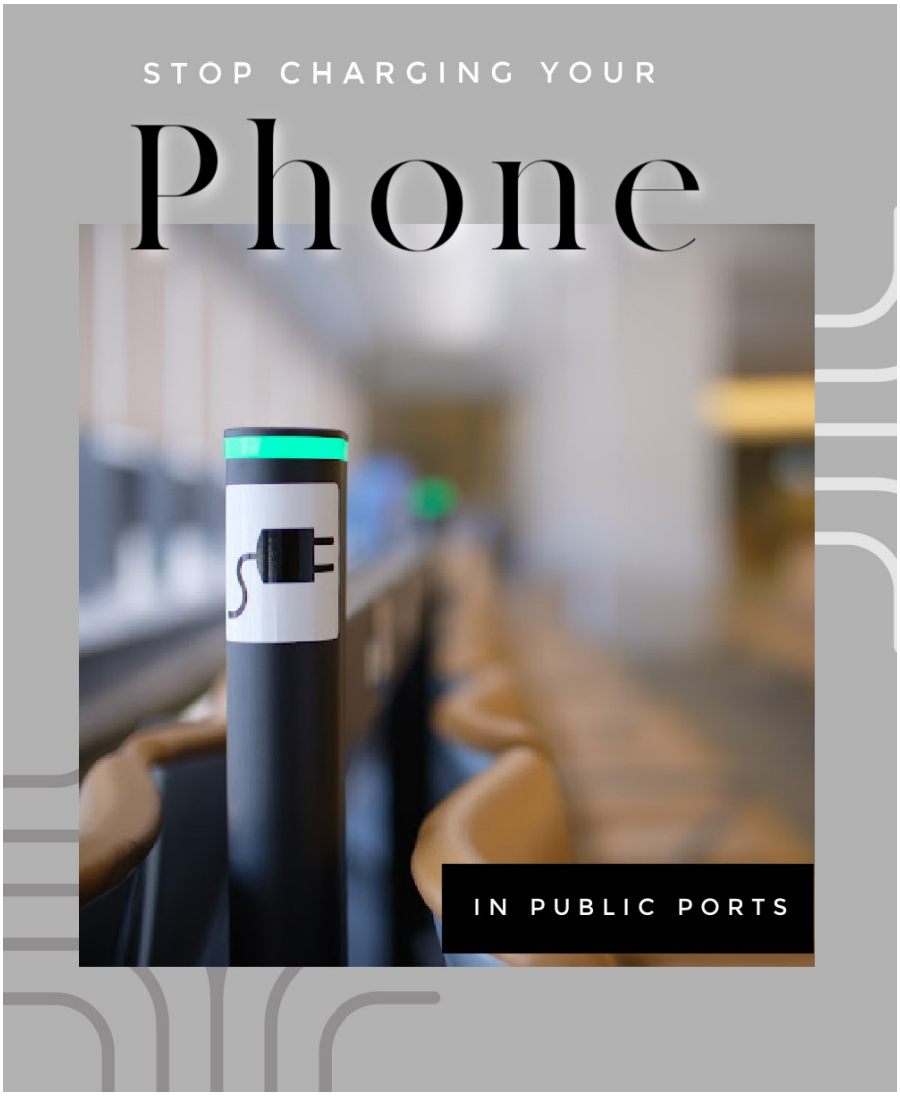
Be aware of friend's account that have already been compromised by an attacker.

You may receive a message from your friend about an unusual promotion, a message that you've been tagged in a post, encouraging you to check it out. This is exactly how most phishing scams spread. If you come across phish-like behavior, report it to phish@fb.com.

Facebook has an enormous third-party app ecosystem. You may have added an app to take advantage of a promotion or contest, played a game, or added new functionality such as music streaming. In most cases, it just means that the app developer has access to some of your profile data. In the worst-case scenario, a malicious developer behind the service can use your account to send out spam. Perform an audit on your account by turning off third-party app permissions. To do this, go to your Facebook Settings, select Apps and Websites, then review the apps and websites that are active on your account. If you see any unwanted third-party apps, you can select them and click "remove".



"For security purposes, the information should make no sense at all to spies and hackers. We'll bring in someone later to figure out what you meant."



We all know that feeling; your battery is low, but you just have to post that status update!

Maybe you just got to the airport and your phone is dead, but you have to get an Uber—so what do you do?

You see a USB port in a public place and of course you're going to plug in your device so you can feel the sweet relief of your phone charging.

Unfortunately, that comfort could be shattered by an invisible attacker collecting information while your phone is plugged into a hacked port, compromising all your data.

Public charging stations and Wi-Fi access points are found in places like airports, planes, conference centers, malls, and parks to name a few, making sure people can always have access to their phones and data.

But, connecting your phone to an unknown port has its risks. The cord you use to charge your phone, is also used to send data from your phone to other devices. For instance, when you plug your smartphone into your computer with the charging cord, you can download photos from your phone to your computer.

If a port is compromised, there's no limit to what information a hacker could take. That includes you emails, text messages, photos, and contacts. It's called "juice jacking". Using hacked ports and your phone's video display, hackers can record everything you type and look at. Despite the risks, public charging stations are extremely popular, often times—there's not even an open port for you to use...but that's not a bad thing.

Instead of charging in public, invest in a portable USB battery-pack. You can also buy USB cords that are specifically meant for charging and cannot transfer your phone's data. The best way to avoid falling victim to juice jacking is to not use public USB ports but instead, rely on your own personal charger.

8 Tips to Make Your Passwords as Strong as Possible

We've been on the internet for almost 35 years, yet we still haven't learned our lesson about online passwords. According to a recent security study, the most commonly used web passwords are things like "123456" and "password." Sure, they're easy to remember, but that makes them just as easy to hack. And if you use that simple password across multiple accounts—as a reported 92 percent of online users do—that puts all of your data at risk. Here are eight tips for ensuring your passwords are as strong as possible.

1. MAKE YOUR PASSWORD LONG.

Hackers use multiple methods for trying to get into your accounts. The most rudimentary way is to personally target you and manually type in letters, numbers, and symbols to guess your password. The more advanced method is to use what is known as a "brute force attack." In this technique, a computer program runs through every possible combination of letters, numbers, and symbols as fast as possible to crack your password. The longer and more complex your password is, the longer this process takes. Passwords that are three characters long take less than a second to crack.

2. MAKE YOUR PASSWORD A NONSENSE PHRASE.

Long passwords are good; long passwords that include random words and phrases are better. If your letter combinations are not in the dictionary, your phrases are not in published literature, and none of it is grammatically correct, they will be harder to crack. Also do not use characters that are sequential on a keyboard such as numbers in order or the widely used "qwerty."

3. INCLUDE NUMBERS, SYMBOLS, AND UPPERCASE AND LOWERCASE LETTERS.

Randomly mix up symbols and numbers with letters. You could substitute a zero for the letter O or @ for the letter A, for example. If your password is a phrase, consider capitalizing the first letter of each new word, which will be easier for you to remember.

4. AVOID USING OBVIOUS PERSONAL INFORMATION.

If there is information about you that is easily discoverable—such as your birthday, anniversary, address, city of birth, high school, and relatives and pets names—do not include them in your password. These only make your password easier to guess. On that note, if you are required to choose security questions and answers when creating an online account, select ones that are not obvious to someone browsing your social media accounts.

5. DO NOT REUSE PASSWORDS.

When hackers complete large—scale hacks, as they have recently done with popular email servers, the lists of compromised email addresses and passwords are often leaked online. If your account is compromised and you use this email address and password combination across multiple sites, your information can be easily used to get into any of these other accounts. Use unique passwords for everything.

6. START USING A PASSWORD MANAGER.

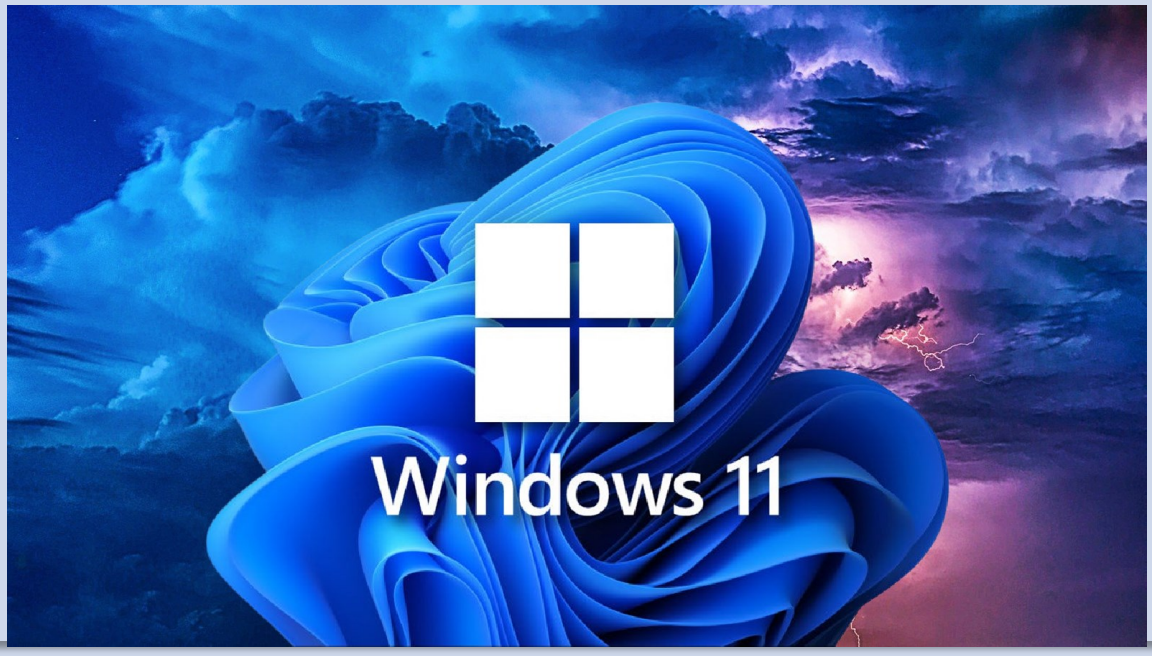
Password managers are services that auto—generate and store strong passwords on your behalf. These passwords are kept in an encrypted, centralized location, which you can access with a master password. (Don't lose that one!) Many services are free to use and come with optional features such as syncing new passwords across multiple devices and auditing your password behavior to ensure you are not using the same one in too many locations.

7. KEEP YOUR PASSWORD UNDER WRAPS.

Don't give your passwords to anyone else. Don't type your password into your device if you are within plain sight of other people. And do not plaster your password on a sticky note on your work computer. If you're storing a list of your passwords—or even better, a password hint sheet—on your computer in a document file, name the file something random so it isn't a dead giveaway to snoopers.

8. CHANGE YOUR PASSWORDS REGULARLY.

The more sensitive your information is, the more often you should change your password. Once it is changed, do not use that password again for a very long time.



Windows 11 is arriving in just a few days, bringing big changes from Windows 10.

With Windows 11, Microsoft has realized Windows should be a powerful desktop operating system. From improved multi-window multitasking and better support for multiple monitors to PC gaming improvements and a Store featuring traditional Win32 desktop apps, Microsoft is embracing the reality of the PC—and making it better. Microsoft has revealed that it will start offering Windows 11 on October 5, 2021.

You won't necessarily be able to get it on that date: "Following the tremendous learnings from Windows 10, we want to make sure we're providing you with the best possible experience. That means new eligible devices will be offered the upgrade first." In other words, Microsoft doesn't want a repeat of the Windows 10 rollout where some apps and hardware simply didn't work with the new OS and caused plenty of grief.

This time around, the rollout "will be phased and measured with a focus on quality". The company says it expects all eligible devices to be offered the free upgrade by mid-2022, and that it will use "intelligence models' that consider hardware, reliability metrics, age of device and other factors. So don't be surprised if you don't see a pop-up giving you the option to upgrade from Windows 10 on October 5th. You should, however, start to see laptops and PCs running Windows 11 beginning to be sold from that date.

Windows 11 features

There are improvements across the board in Windows 11, with Microsoft promising that updates will be 40% smaller, and touting Windows 11 as "the most secure release yet". There's even an estimated installation time for Windows Update, so you can see whether you need to hold off from updating your PC until later in the day.

In terms of cosmetic improvements, Windows 11 is a big upgrade. It comes with a new Start Menu, Fluent Design elements, new inbox apps, rounded corners and more. In addition to these design overhauls, Windows 11 also comes with a new File Explorer and Settings app.

File Explorer is getting a new header menu, modern context menu and minor improvements. On the other hand, the Windows Settings app has been completely redesigned with a new layout optimized for all form factors, and it also comes with new customization options.

New multitasking features are also on offer thanks to a feature called Snap Layouts, which enables you to arrange multiple windows across the screen, not just side by side, but in columns, sections and more.

Another feature is Snap Groups, where you can go back to previously snapped windows from the dock, so for example you can go to your email app, Edge browser windows or anything else without having to snap them back to the previous view again.

There's also improved multi-monitor support, so when you reconnect an external monitor, Windows 11 remembers the previous positions of the windows that were on that monitor.

There's now a much-improved health check app found in Settings, where Windows 11 will recommend you to turn down the brightness for example, change the power saving mode of the battery and much more.

client testimonials

We were referred to PCS when a trusted advisor observed that we had a fragmented IT solution. PCS brought a more comprehensive view, and a value proposition that aligned with our interests, and their execution has been fantastic.

PCS is a great fit for us because of their entire business model. PCS is relationship focused, and has a proactive approach to managed services that allows us to focus on our core business and expertise.

PCS is a great partner and acts as an extension of our company, like a virtual IT department. While we considered creating an internal IT position, we decided that having a team of IT experts that PCS brings was more valuable. By using PCS we have achieved a better service at a lower cost than we would have internally, or compared to the peers we evaluated.

Sam DiCicco Jr.
DiCicco Development, Inc.

The average computer user blinks just 7 times per minute.

As we stare at the computer screen or while reading, our blink rate decreases. The average blink rate is 20, so this is why your eyes dry out more while working in front of your computer screen. This will cause your eyes to feel dry and to burn.

Other Symptoms:

- Eye fatigue
- Light sensitivity
- Blurred vision
- Headaches

Staring at a screen all day can cause memory loss, brain fog, insomnia, vision stain, and headaches. And sitting all day can lead to obesity, and high blood pressure or blood sugar, among other things. Fortunately, there are some things you can do to actively prevent any of that from happening:

Protect your eyes::A computer screen can seriously impact your vision, but it’s not a lost cause. Make sure to take blinking breaks. Become aware when you are not blinking enough and try to blink more frequently. Take a vision break every 20 minutes or so. Look at something about 20 ft. away for 20 seconds.

Blue light glasses are also helpful for preventing eyestrain.

Poor positioning of your monitor can make it difficult to focus on the screen. A suggestion to find relief is to sit arm's length away from your computer. Being too close to the screen can make it worse. You may find it helps to change the contrast and adjust the brightness on your screen, along with avoiding any glare from various sources.

- Large monitors are easier to see, font size can be increased
- Flat screens have less glare
- Controlling the brightness and contrast will reduce eye strain and decrease focusing demand
- Keep your screen free of dust and smudges

More Tips for Staying Comfortable at Your Desk

In addition to all the eye issues just mentioned, sitting all day can lead to obesity, and high blood pressure or blood sugar, among other things. Fortunately, there are some things you can do to actively prevent any of that from happening:

- **Adjust your posture:** If you're constantly looking down, you're going to be hunching forward and straining your neck. It's easy to get into a slumped posture when you're sitting for hours on end. Focus on sitting up straight (set an alarm to remind yourself if needed) or use a pillow for more support. Footrests can also help you sit up straight and, generally, just make you more comfortable.

- Take walking breaks: As we already mentioned, sitting all day can be detrimental to your physical health. Set a timer and, at least once every hour, get up and walk around. Do a few laps around your office or the building. You might also want to consider getting a standing desk to avoid sitting all day.

- Fix your desk setup: There are many ways you can make you desk or office a little more Zen. For example, if you work from home, you can add a diffuser or humidifier to clear the air and help you breathe better. You can also add some plants to enhance your mood, or get rests for your wrists, pillows for your chair, and so on. Anything that makes you feel more comfortable will help.

- Stay hydrated: Drinking water is just good for your health all around, so it's always a good idea to keep some handy. It also forces you to get up often and walk to the bathroom, so it's a win-win.