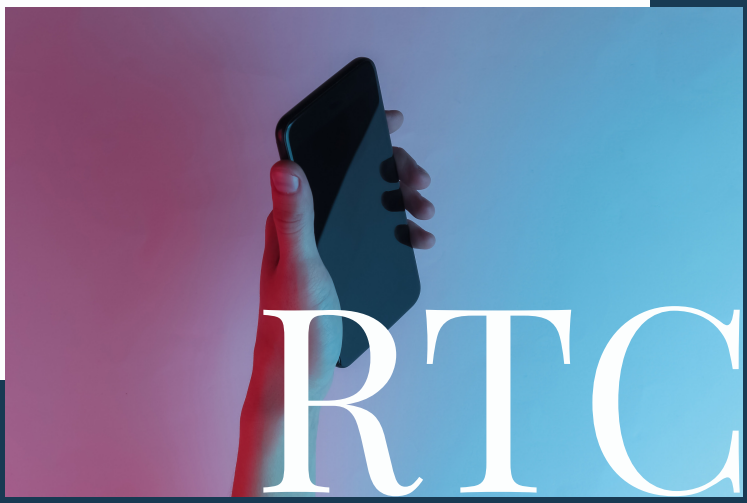



# PROTECTING YOUR SMARTPHONE

January 2023


https://righttoconnect.org

# Protecting Your Smartphone

## Apply for a VPN

Primarily avoid connecting to unsecured public Wi-Fi networks if you can and do not need them. By any chance, if you connect privately on insecure public networks like airports, cafes, and hotels, use a VPN because it hides your connection from hackers. Your communication and personal and professional business data on your smartphones are safe from eavesdropping with a VPN connection.


## Provide an extra safety layer

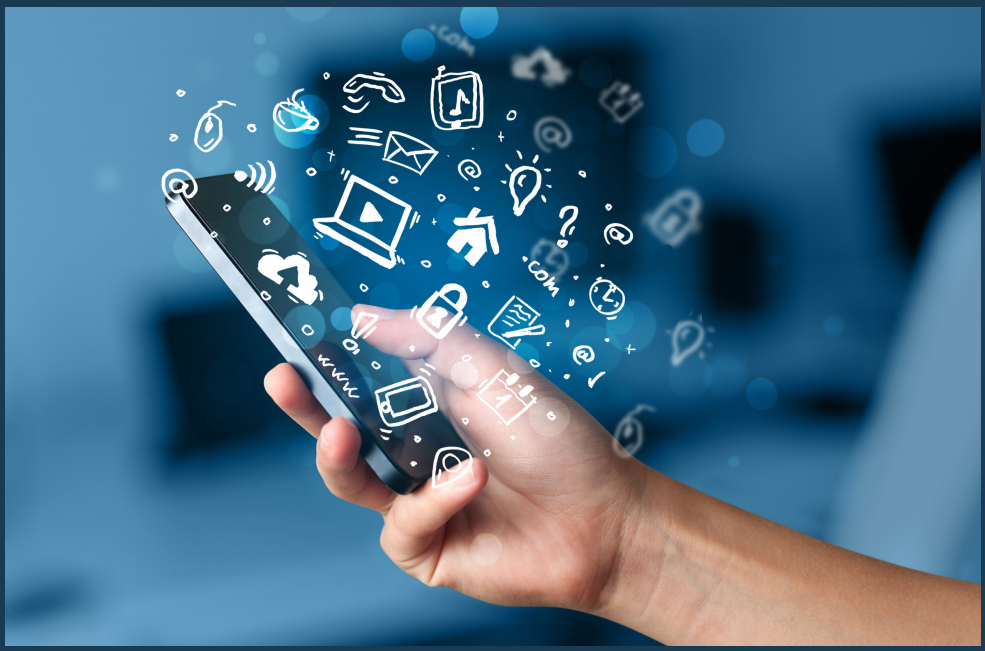
To provide an extra layer of safety to your smartphone, use your face, finger, pattern, or PIN. Using a facial ID, a fingerprint, a pattern, or a pin will help you if your smartphone is stolen or lost. For your privacy protection, utilize two-factor authentication on the apps and use a strong password for your smartphone and the Apps.

# Get apps app only from official app stores

Both Apple's App Store and Google Play have safeguards in place to help stop potentially harmful apps from entering their shops. Outside of the app stores, malicious programs are frequently found. These apps can operate in the background and compromise your personal information, including passwords, credit card details, and nearly everything else you keep on your smartphone.

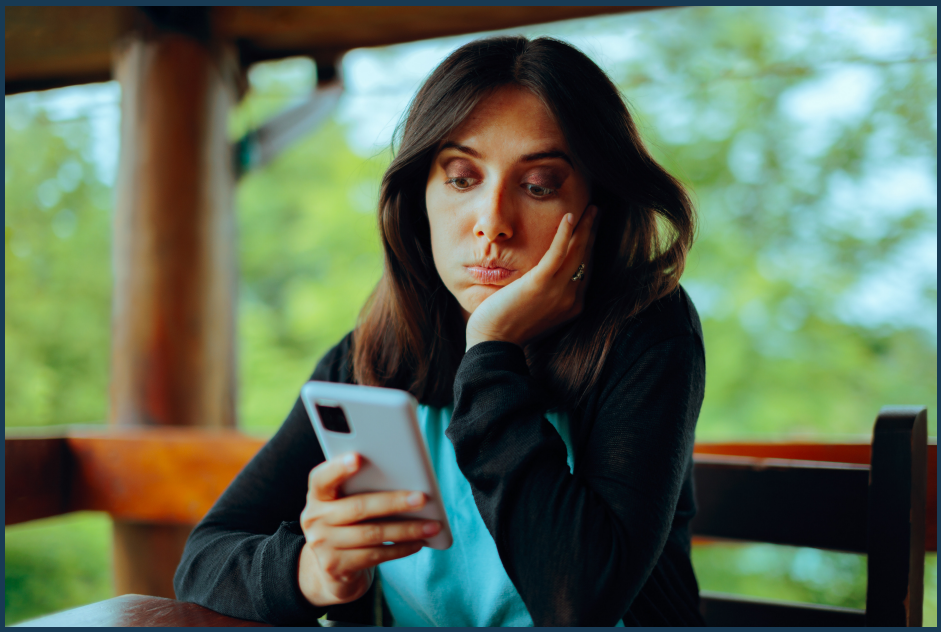
## Know how to remotely lock or wipe your phone in an emergency.

If your phone is lost, lock it remotely or even completely delete all of its data. The last part about erasing the phone may seem like an extreme measure, but if you make frequent backups, as indicated above, your data is safe in the cloud and available for restoration. If you can wipe your smartphone remotely, hackers won't be able to access important information about you or your organization, which can help you stay out of trouble and keep your professional endeavors secure.



## Remove apps that are out of date

Update the ones you decide to use them. If you remove apps, there are some apps that come with accounts and may have stored your data from your smartphone. Before deleting these apps, make sure to destroy your data and then deactivate your accounts.



If you don't update an app, it could be affected by a security flaw. Getting rid of outdated apps is a wise decision in an era of data leaks and dangers. For the ones you do maintain, make sure to update them frequently and enable auto-updates.

# Keep your phone safe by using security software

Installing security software on your phone can protect you and the documents. Mobile security software helps keep your data, payments, and shopping secure whether you are using iOS or Android.


# Get a backup of your phone's data

Back up your smartphone's data will help you switch to a new phone easily by transferring your data from the cloud to your new device. Moreover, if you lose your phone and or if it is stolen and or destroyed, it guarantees that your data will still be with you. You can easily back up your iPhones and or Android devices.
Hackers install fake access points—connections that seem like Wi-Fi networks but are traps—in high-traffic public places like coffee shops and airports. Cybercriminals give access points to well-known names like "Free Airport Wi-Fi" or "Coffeehouse" to encourage consumers to log in. To access these free services, attackers even require you first to sign up for an "account," complete with a password.

# Phishing attacks

Most phishing attacks target mobile devices since they are always on. Mobile users are especially exposed because they routinely check their email in real-time,


reading and opening emails as they come in. Mobile email programs display less information because of the smaller screen sizes, which leaves consumers more exposed. Links in emails you don't recognize should never be clicked. If the issue is not urgent, let the answer or action items wait until you are at your computer.

# Spyware


Although spyware poses a more immediate threat than malware, many mobile users are worried about malware transmitting data streams back to hackers. Instead of malware from unidentified attackers, users should frequently be concerned about spyware used by partners, coworkers, or employers who want to track their activities.

These apps, often known as stalkers, are commonly designed to be installed on the target's smartphone without their knowledge or agreement. Thus, a comprehensive antivirus and malware detection package should employ specific scanning methods.

## SMiShing

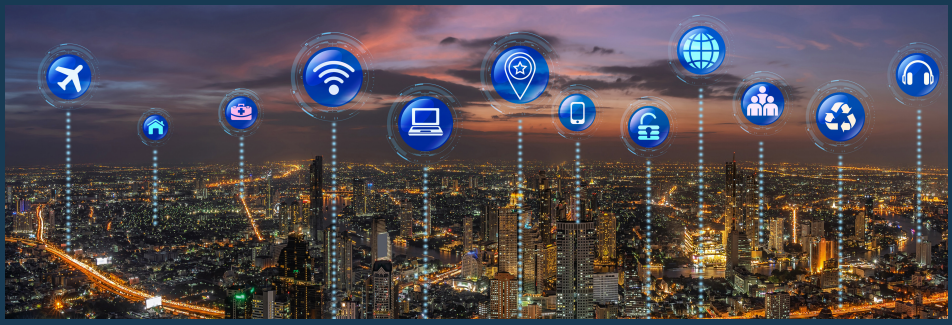
Cybercriminals aim to trick users into downloading malware, clicking on dangerous links, or disclosing personal information by using SMiShing, a tactic similar to phishing scams. A SMiShing assault is launched through text messages as opposed to email.


## BYOD

As corporate users now have high-level access to personal mobile devices, cellphones and tablets are virtually replacing desktop PCs for many businesses. However, unlike the desktop PCs that they are replacing, personal mobile devices don't offer the same level of integrated security or control.

# The Internet of Things (IoT)


Users and antivirus software may not always be able to keep a watch on smart gadgets due to their rapid expansion in number, from RFID chips to thermostats and even home appliances. IoT devices are, therefore, a sought-after target for hackers who use them as points of entry into larger networks.



# Resources:

https://nordpass.com
https://www.keepersecurity.com
https://www.roboform.com
https://www.dashlane.com
https://1password.com
https://www.lastpass.com
https://www.keepsolid.com/passwarden
https://www.bitdefender.com
https://ca.norton.com
https://www.totalav.com
https://surfshark.com
https://nordvpn.com