TKS Helpful Information: What to do if your phone is lost or stolen

A lost phone, or worse, a stolen phone is a terrible thing – but it is a real risk and can definitely happen. According to statistics, 19 million phones are lost or stolen each year, and traveling puts you at an even higher risk theft. You can avoid a total disaster if you prepare properly and don't panic when your phone goes missing. Most importantly, don't wait until it's too late. Know what to do if your phone is lost or stolen so you can recover faster, protect your identity, and not lose all those great vacation photos!

Use these tips to be prepared and protect your data and then, if you do lose your mobile phone, to act quickly.

How to prepare for the day you lose your phone.

A little preparation goes a long way to not only reduce anxiety, but to protect your data and make transition to a new device relatively simple.

Here are some steps that you can take to ensure your phone stays safe, whether it's in your pocket or in some stranger's:

- If you can turn on your device or open the home screen without using a password or fingerprint, you're tempting fate! Ensure that your personal data stays secure no matter who's holding your phone by setting up your device to **require a password every time you turn it on or open it**. Secure the phone with a strong PIN or password and use a biometric option, such as a fingerprint scan, whenever possible and remember, the stronger the password the better!

- Make sure your smartphone knows you. You can set up both Android and iPhones to know your emergency contact information. Many do this in the initial setup process, but it is a good idea to **double check the information**, just to be sure. (Android: Settings>Security>Owner Info. iPhone: Add emergency contact info in the Health app, Medical ID page. Also check Settings>Mail, Contacts, Calendars>My Info to ensure you're listed as the owner of your phone.)

- Register your phone for location tracking. Both Android and iPhone provide options to locate a device, and some mobile antivirus software includes this option. When registering, you will need to create an account to enable access to the service from another device. Make sure these credentials are memorable.

- Any data on your phone should be backed up to the cloud. Then, if the device does go missing, your important information, photos, music and other data will be easily recoverable from another device.

- Always log out of apps when you aren't using them, especially those for Facebook, Twitter, and other social-networking services.

- Keep a list of important information that you keep stored on your phone, such as your carriers information, bank accounts, important phone numbers and addresses, digital wallet balances, or frequent-flyer and travel details, especially if this information isn't readily available elsewhere in a place that you can access without your phone.

TKS Helpful Information: What to do if your phone is lost or stolen

Steps to follow if your phone is lost or stolen:

Step 1: Call & Text your phone:

When your phone goes missing, don't panic. The first thing you should do is to determine if the phone is really lost – or just misplaced. Once you realize your phone is missing, immediately use another phone to call and text your number. It is a good idea always to leave a voicemail and text message on your missing phone with current contact information and a call-back number. This easy trick can help a Good Samaritan get your phone back to you.

Step 2: Find-My-Phone:

The find-my-phone feature is available on both iPhone and Android and can help recover a lost or stolen device. If you have this feature turned on or installed, you'll be able to see where the phone is remotely by logging into your Apple or Google account on another device. You'll also be able to remotely trigger a sound alert on your phone. If you have Family Sharing with Apple, other users on your account will be able to see where your phone is. If the phone is off or offline, tracking unfortunately is not available.

Step 3: Contact your mobile carrier:

Report your missing phone to your network provider
You should notify your network provider ASAP if your phone is lost or stolen, so they can block it and stop anyone else from using it. If you don't notify your provider immediately, you will have to pay for any unauthorized phone calls, which can be very expensive. If your phone has been stolen, ask your provider for the phone's identification number (IMEI) - you'll need to give this information to the police.

Don't worry if you do find your phone, your provider will be able to reactivate it.

Step 4: Alert the police:

You should report a stolen phone to local police as soon as possible. Your network provider will give you your device identification number (IMEI), which you should pass on. Be sure to note the police reference number because in most cases a police report is required if you need to protest fraudulent charges made with your device, or if you plan to file an insurance claim.

Step 5: Remote - wipe the device:

If you can't track your phone, or you know that it has been stolen, you should wipe its data. Though it will mean losing any data that you have not backed up, it is the best way to ensure your identity and personal data is protected. You can wipe your phone remotely within the find-my-phone app on both iOS and Android. If your device is offline when you perform a remote erase, the erase will occur when the phone is turned back on.

TKS Helpful Information: What to do if your phone is lost or stolen

Important Note for Apple Users: Once you erase your phone, it can no longer be tracked. If you try and remove your device from your Apple account while it's offline, it will reappear in Find My iPhone. If you remove your device from your Apple account while the phone is online, the activation lock will be turned off, which means another person could activate the phone.

Step 6: Lock your device:

With the latest iOS update, Apple included a feature called Lost Mode that will remotely lock your device with a passcode and display a custom message on the lock screen. This mode can also suspend the ability to make payments via Apple Pay.

Step 7: Change your passwords

Even if you wipe your phone, you should also immediately change your passwords for critical apps such as email, cloud storage and any other accounts or apps that are downloaded to your phone, for example online banking, or airlines. If you have credit cards attached to any apps such as Apple Pay, or Spotify for example, be sure monitor them for suspicious activity.

Step 8: Contact your bank and credit card companies:

If you believe that sensitive information is at risk, treat your lost phone as you would a lost or stolen wallet. Contact your banks and credit card companies about potential theft resulting from the loss of your phone.

Step 9: Notify your employer:

If you use your device to access work emails, apps, or just text colleagues about work-related topics, inform your employer. This allows your firm to take preventive steps to secure its data. Your company's IT department may also be able to delete sensitive company data from your phone remotely.

Step 10: Getting a replacement SIM card and phone:

Your network provider will not replace your phone free of charge and you will have to continue to pay your monthly service fee (and hardware installment plan when applicable) until the end of your contract.

Your network provider will be able to supply you with a replacement SIM card for a one-time fee. When you have purchased a new phone, simply insert the replacement SIM into the device and resume using your service.