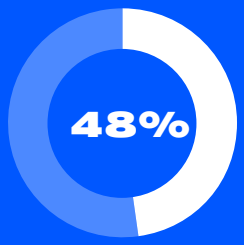
PRACTICE GOOD CYBER HYGIENE

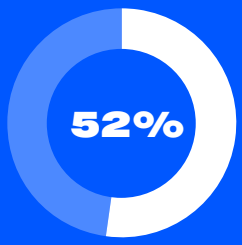
9 ESSENTIAL STEPS TO KEEP YOUR DEVICE SECURE

Practicing good basic cyber hygiene is one of the best, and easiest, ways people can protect themselves from cyber criminals and others that mean you harm. Experts estimate that over 80% of cyber incidents could have been stopped if the targets had adopted good cyber hygiene practices. Adoption of basic and widely recognized cyber hygiene best practices can be one of the first and most important defenses people can employ to better protect themselves from ever-evolving and increasing cyber threats. This involves simple steps like adopting strong passwords, using multifactor authentication, updating devices when updates are issued, only downloading from official app stores, and avoiding untrusted links.

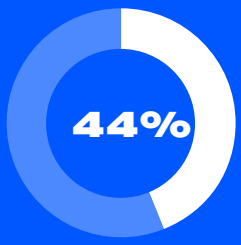
But according to a recent consumer survey commissioned by Trusted Future and conducted by the research firm AudienceNet, only about half of respondents take these recommended steps.



Adopting 2-factor authentication



Avoiding untrusted links



Only downloading from official app stores

Keeping software up to date

LOCK YOUR DIGITAL DOORS

REUTERS

One password allowed hackers to disrupt Colonial Pipeline, CEO tells senators

Bloomberg

Hackers Breached Colonial Pipeline Using Compromised Password

The hackers behind the intrusion into Colonial Pipeline's IT systems, which led to panic buying at gas stations, were able to gain access to the company's systems because one of Colonial's employees reused a password from another account. Once that other account was compromised, hackers were able to identify the employee's password in a batch of leaked passwords posted to the dark web.

BBC

Flubot: Warning over major Android 'package delivery' scam.

Taking advantage of the surge in online deliveries during the pandemic, hackers sent text messages to millions of mobile phones prompting users to download a parcel tracking app, which was actually loaded with the "Flubot" malware. Because the app was not on the official Google Play Store, Android devices were only vulnerable if the user changed the default security settings to allow sideloading. Users who did not reverse the default setting of no sideloading stayed secure.

01

USE STRONG AND UNIQUE PASSWORDS FOR EACH ACCOUNT.

Use strong passwords or passphrases, don't use the same password for multiple accounts, and pay attention to any notice from a legitimate source that your password and username have been found on the 'dark-web' and then change the password for that account. If you use the same password on multiple accounts and it becomes compromised, a criminal could try that password on your other accounts. Don't make it easy for people looking to steal from you!

02

USE A PASSWORD MANAGER.

Password manager programs can help you create complex passwords for each of your accounts, remember those passwords, and even notify you if one of your passwords is found in a data leak.

03

USE MULTI-FACTOR AUTHENTICATION.

Multi-factor (often called two-factor) authentication can double your login protection by creating a second requirement to get access to your account. Even if your username and password are stolen, criminals won't be able to access an account protected by two-factor authentication because the second factor (such as one sent to you via the SMS messaging function on your mobile device) would not be known to the criminal. It's simple to use, turn it on!

04

AVOID INSECURE WEBSITES.

Only visit websites that use HTTPS (check the beginning of the website's URL and look for the image of a lock) to protect your browsing from prying eyes – especially if using public Wi-Fi.

05

ONLY DOWNLOAD FROM OFFICIAL APP STORES.

Mobile malware is on the rise—a recent report from Nokia found an 80% increase in "banking malware" targeting smartphones in the first half of 2021. Mobile apps are the main way hackers distribute malware, ransomware, adware, and other malicious software. Official app stores, such as Android's Google Play and Apple's App Store, invest considerable resources into vetting apps to better protect you. Malicious apps are also regularly pulled from the two stores when they are discovered. Users that "sideload" apps from unofficial stores and third-party websites are much more likely to have their device infected by malware.

06

KEEP YOUR SOFTWARE UP TO DATE.

Always install official security updates from your device or software supplier. Criminals are constantly finding new ways to try to access your device or information, and technology companies are constantly updating your protections. A security update means your provider is plugging another hole—but you must install the update to get that protection! If offered, turn on the function that automatically updates your device.

THINK BEFORE YOU CLICK

07

RESPOND TO UNSOLICITED MESSAGES WITH CAUTION.

From the early days of the Internet, cybercriminals have used phishing and other "social engineering" tactics to trick victims into voluntarily disclosing account information and other private data or to load malicious software onto their devices. As we use our phones to do more things, and rely on them for more hours of the day, criminals have evolved too and are now using even more clever ways to trick us using text messaging and other communication services. Criminals may attempt to trick you with a personalized message, or use language and branding to make a message look "official," for example from a government agency, company, or other trusted organization. Don't be fooled by personalization, branding, or messaging that looks legitimate.

08

IF YOU ARE UNSURE, DON'T CLICK!

Phishing messages often use links disguised to look legitimate to deliver viruses, malware, and other malicious software. Look for suspicious attachments, poor grammar, and spoofed links. Sometimes it can be hard to determine whether an email is legitimate—when that happens the best approach is to contact the sender directly to confirm that the message is legitimate. If a message says it's from a bank and asks you to click on a link, call the bank. If a delivery service asks you to confirm a delivery, go to the company's website where you placed the order and confirm it from there. You can report spam or scam texts on the FTC's website.

09

BEFORE YOU DOWNLOAD OR USE AN APP, DO SOME BASIC PRIVACY DUE DILIGENCE.

Before you download an app or grant an app permission to access certain data, review the privacy label for the app in the app store to understand what data it collects and for what purposes. Make sure you are confident that you can trust the app to safely handle your data. Does it make sense for this app to access your microphone, contacts, and other parts of your phone? Asking these questions is now easier than ever, as official app stores are now mandating increased privacy disclosures by developers. For more tips on how to safeguard your privacy when using digital devices, review our **Eight Steps to Better Protect Your Privacy Online.**

TRUSTED RESOURCES FOR FURTHER READING

SECURING DEVICES

Federal Trade Comission, *How to Protect your Phone and the Data on It* →

Cybersecurity & Infrastructure Security Agency
- *Cyber Lessons* →
- *Creating a Password* →
- *A How-To-Guide for Multi-Factor Authentication* →
- *Security Tip: Securing Wireless Networks* →

Canadian Centre for Cyber Security, *Cyber Hygiene* →

Australia's eSafety Commissioner
- *Safe passwords* →
- *Managing passwords* →

New Zealand's Computer Emergency Response Team
- *Keeping your mobile phone safe and secure* →
- *Keep up with your updates* →

United Kingdom's National Cyber Security Centre
- *Improve your online security today* →
- *Protecting devices from viruses and malware* →

India's Ministry of Electronics and Information Technology's Computer Emergency Response Team (CERT-In), *Securing mobile devices and applications* →

European Union Agency for Law Enforcement Cooperation (Europol)
- *Safe Teleworking Tips and Advice for Employees* →
- *Make your home a cyber safe stronghold* →
- European Union Agency for Cybersecurity, *What is a password and why it is important* →
- Japanese National Center of Incident Readiness and Strategy for Cybersecurity, *Information Security Handbook for Network Beginners* →

USING APPS SAFELY

Federal Trade Commission, *Tips to Protect Your Privacy on Apps* →

Cybersecurity & Infrastructure Security Agency, *Security Tip: Privacy and Mobile Device Apps* →

Military OneSource, *Top 4 Tips for Cell Phone Safety* →

Australia's eSafety Commissioner, *Being safer with apps* →

European Union Agency for Law Enforcement Cooperation (Europol), *Just a game?* →

SOCIAL ENGINEERING / PHISHING ATTACKS

Cybersecurity & Infrastructure Security Agency
- *Security Tip: Avoid Social Engineering and Phishing Attacks* →
- *Stop Ransomware* →

Federal Trade Commission, *How to Recognize and avoid phishing scams* →

Australia's eSafety Commissioner, *Avoiding scams and tricks* →

Canadian Centre for Cyber Security, *Staying Cyber-Healthy During COVID-19* →

European Union Agency for Law Enforcement Cooperation (Europol)
- *Take control of your digital life. Don't be a victim of cyber scams!* →
- *Ransomware: The Malware that Holds Your Data Hostage for a Price* →
- *Tips & advice to prevent ransomware from infecting your electronic devices* →

National Cybersecurity Agency of France, *Ransomware Attacks, All Concerned: How to Prevent Them and Respond to an Incident* →

USEFUL CYBER SAFETY TIPS

The New York Times, *How to Protect your Digital Privacy* →

CNET: *7 data privacy tips for your phone from digital security experts* →

National Network to End Domestic Violence: *Best Practices When Using Mobile Devices* →

Norton: *Good cyber hygiene habits to help stay safe online* →