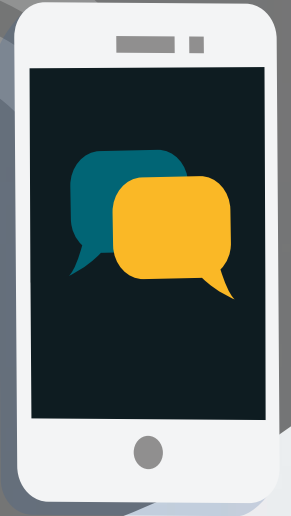


## Smartphone Security Threats

Phone hacking can compromise your identity and privacy without you even knowing. Even with 2 Factor Authentication and Face Recognition technology we're at risk



290 million Americans now own a smart phone, 85% of the population. That's up from 35% just ten years ago!

Increased use for business, developments in technology, apps, data storage and functionality mean that our mobile device is a key life tool. We have lots and lots of information stored on or connected to our smartphones.

A recent study showed that we value our mobile device and its data at \$14,000!

These developments bring threats to our security and our information from hackers and identity thieves.....let's take a look

## Signs That Your Phone May Have Been Hacked



Your phone loses power quickly



You're getting multiple unfamiliar calls or texts

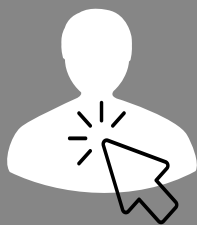


Your phone runs very slowly



You're being asked to reset passwords or sign in verifications for other online accounts

## Common Ways our Device & Info are Compromised



### Social Engineering

Personalized phishing and smishing attacks trying to trick you into giving up information or accepting downloads and attachments.



### Malicious Apps

A huge percentage of mobile apps are largely unsecured and when we download them we generally give "permission" for the app to access files on our device. Rogue actors exploit these access points.



### Spyware

Spyware is used to survey or collect data and is most commonly installed on a mobile device when users click on a malicious advertisement or through scams that trick users into downloading it unintentionally.

# How Can We Protect Ourselves?

- **Back Up Your Data Regularly.** If you do have your phone hacked/stolen you'll want to be able to remotely erase it. That means you need to have the content backed up and stored elsewhere
- **Don't Download Unknown Apps.** Look at reviews and research before installing if you are unsure. If you're not confident in safety of an app, do not install it.
- **Don't Click on Unknown Attachments.** It's the most common way to unknowingly download malware
- **Don't Jailbreak Your phone.** While it allows you to download from unofficial app stores, it increases risk of unknowingly getting hacked. Aside from malware or spyware, this means you'll miss security patches in the latest updates. This makes your risks of being hacked even higher than normal.
- **Keep Your Phone With You At All Times.** Physical access is the easiest way for a hacker to corrupt your phone. Theft and a few hours of effort could result in your phone being breached. If you can keep your phone with you, a hacker will have to work much harder to get into it.
- **Always Use a Passcode Lock and Use Complex Passwords.** Do not use easily guessable PINs, like birthdays, graduation dates, or basic defaults like "0000" or "1234."
- **Don't Store Passwords On Your Device.** Remembering unique passwords for every account can be difficult. So use a secure password manager instead.
- **Frequently Clear Your Internet History.** It can be simple to profile trends about your life from all the breadcrumbs of your browser history.
- **Enable a Lost Device Tracking Service.** If you lose track of your device out in public, you can use a lost device finder to trace its current location. Some phones have a native application for this, while others may need a third-party app to add this feature.
- **Keep All Apps Up to Date.** Even trusted apps can have programming bugs that hackers exploit. App updates come with bug fixes to protect you from known risks.
- **Always Enable Two-Factor Authentication (2FA).** This is a second verification method that follows an attempt to use your password.
- **Be Cautious About Using Text or Email For Your 2FA.** Text message and email 2FA are better than no protection but might be intercepted through hacks like SIM swapping.
- **Don't Use Public Wi-Fi Without a Virtual Private Network (VPN).** Get a VPN Secure Connection encrypt and anonymize your data so unwanted viewers can't see it.

To learn more about this complex issue and download the Infographic, click on the button!

[Smartphone Security Info](#)