PROTECT YOURSELF

Help Protect Your Phone from Cyber Attacks

Phones are a great target for theft and hacking. Here's help to avoid five top threats.

FOR BETTER OR WORSE, OUR LIVES ARE TIED TO OUR PHONES. The way we use them—constantly, automatically, distractedly—makes them excellent potential targets for fraudsters. One of the best things you can do to help protect your phone is to just be more aware when you're using it. To that end, we've outlined five mobile security threats to keep in mind, and what you can do to help avoid them.

THREAT: **PHISHING**

How it works: You get a text message with a link to review a recent order from an online store. You tap the link and try to log in but are unsuccessful. You try again and you see your order. Everything looks fine, so you forget about it. Unfortunately, the text and the first login page were a fake, and your login credentials have been stolen.

Phishing is the most common cyber threat and can happen in any messaging platform. In fact, 83% of successful mobile phishing happens outside of email[†]. Fraudsters build near-perfect replicas of real emails, messages, and websites to fool us (the most commonly impersonated companies are Facebook, Apple, and Google[‡]).

What you can do:

- ☐ Be suspicious of any message, email, or text with a link in it, especially from someone you don't know.
- ☐ If it's an email, try to look at the actual address of the sender (not just the name, which is easily faked).
- ☐ If anything looks off, close the window and go to the website directly.

THREAT: **VISHING**

How it works: You get a call from someone at the Social Security Administration who says there's been legal action against your social security number. They seem to know a lot about you, so you answer the questions and confirm your social security number.

Just as with phishing, everything about the call seemed legitimate but it was fake. Even the phone number can be made to look like it's from your area code. Often, the caller will paint an urgent scenario. Just last year, the government broke up a vishing-style IRS scam that took in hundreds of millions of dollars over four years.[§]

What you can do:

- ☐ Never give out personal information before validating who you're giving it to. Always look up the real customer service number and call back to verify that the caller and the reason for the call were legitimate.
- ☐ Check out the Federal Trade Commission's website, consumer.ftc.gov/features/scam-alerts, which tracks recent known scams (including the social security one above).

THREAT: **PHYSICAL THEFT**

How it works: You set your phone down on the table at a busy cafe, open a magazine, and five minutes later your phone is gone.

Cellphone theft actually appears to be declining in some places in recent years, perhaps due in part to improved tracking and remote locking tools now common in phones[‖]. But that doesn't mean the threat is gone. A phone that can be unlocked is a treasure trove of information. Even a wiped phone can be sold for parts.

What you can do:

- ☐ Be vigilant: keep your phone in your pocket or purse.
- ☐ Turn on Find My iPhone (Apple) or Find My Device (Android), so you can locate and lock or erase your phone from afar.
- ☐ Require a passcode, thumbprint, or face scan to unlock the phone.
- ☐ Enable the setting that will erase the phone after a set number of failed login attempts.

THREAT: **ROGUE APPS**

How it works: A message on WhatsApp says you've been selected for access to a "golden" version of the app, along with a link for installing it directly. Unfortunately, the app you're installing is a fake version containing code that captures your login and other data as you use it.

This is a real example of what's called a repackaged app, in which "a hacker takes the original app, reverse engineers it, and injects his malicious code," according to Asaf Ashkenazi, chief strategy officer at security provider Inside Secure. Google has removed thousands of these repackaged apps from the Google Play store[#], and they have even appeared in the iOS app store[††].

What you can do:

- ☐ Make sure you only download applications from a reputable app store.
- ☐ Even in official app stores, pay attention: read reviews and descriptions; make sure the name is spelled correctly.

THREAT: **MAN-IN-THE-MIDDLE ATTACKS**

How it works: At a coffee shop, you join the first open Wi-Fi network you see. Unfortunately, that network was set up by a fraudster and can capture your data as you surf the web.

These types of attacks are most common in public places, where hackers can cast a wide net, and are very hard to detect. Even if you're using https sites—which means the data going back and forth is encrypted—a rogue hotspot can fake that encryption and still grab the information flowing through it.

What you can do:

- ☐ Avoid open Wi-Fi networks and use your cellular data connection instead.
- ☐ If you must jump on Wi-Fi, pay attention to the network you join, and avoid doing any sensitive surfing or transactions.
- ☐ Use an app instead of a browser whenever possible.

Tools to help avoid fraud

Huntington has tools that can help mitigate some of these cyber risks, including alerts*, which can let you know about unusual or suspicious account activity so you can catch fraud early, and the ability to lock your credit or debit card if it is lost or stolen.

Contact Huntington

If you think you may be a victim of fraud related to your Huntington credit or debit card, or your card has been lost or stolen, please call us at **(800) 480-2265**.

Visit **huntington.com/Security** for additional information.

**Carrier message and data rates may apply.*

---

† Wandera, *Understanding the mobile threat landscape*, 6.
‡ Ibid., 7.
§ Hauser, Christine. "U.S. Breaks Up Vast I.R.S. Phone Scam." *The New York Times*, July 23, 2018.
‖ Mlot, Stephanie. "Cell Phone Kill Switches Prompt 'Dramatic' Drop in Thefts." *PCMag.com*, February 11, 2015.
Ahn, Andrew. "How we fought bad apps and malicious developers in 2017." *Android Developers Blog*, January 30, 2018.
†† Trend Micro, "Masque Attack Abuses iOS's Code Signing to Spoof Apps and Bypass Privacy Protection." *Security Intelligence Blog*, October 31, 2016.