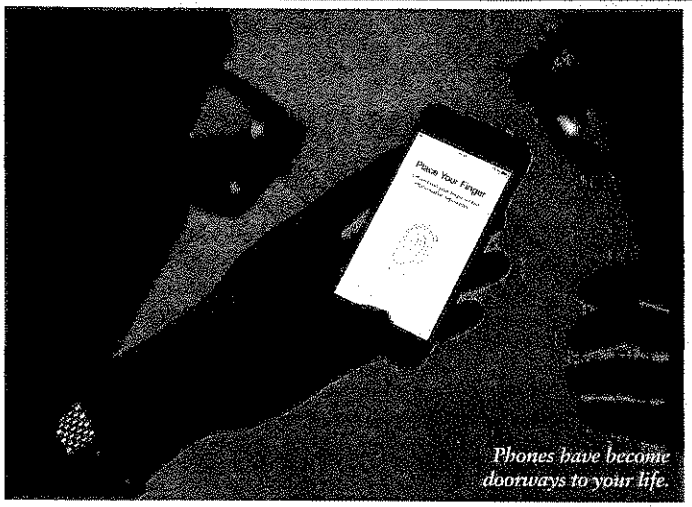

Phones have become doorways to your life.

Keeping hackers out of your phone

The Apple-FBI battle over unlocking an iPhone has raised important questions about mobile phone security.

Do smartphones need to be secured?

Today's smartphones are supercomputers loaded with a vast trove of valuable information about you that hackers and criminals want to steal. Smartphones store data related to your daily life, including texts, email, photographs, schedules, and contact lists. They can also provide direct access to your bank accounts; to your accounts on Facebook, Twitter, and other social media; and to retail accounts like Amazon or iTunes, along with any credit card numbers that are associated with these accounts. If your phone is linked to work computers or email, sensitive business data may be accessible as well. People who don't protect their phones put themselves at risk for hacking, identity theft, fraud, and other cybercrimes. "You can extract enough information on a typical person's phone that you can construct a virtual clone of that individual," Elad Yoran, executive chairman of the communications security company Koolspan Inc., told *Bloomberg.com*. Hackers can even use what they learn about your friends, family, and colleagues to launch attacks on others.

How big a problem is mobile hacking?

It's big and getting bigger. Mobile attacks quadrupled from 2013 to 2014, to nearly 1.4 million attacks, according to cybersecurity company Kaspersky Lab. Consumers in the U.S. lost nearly $30 billion to cybercrime in the past year, security software company Symantec found. And one in five companies has suffered a security breach involving a mobile device, according to Crowd Research Partners. Given that 68 percent of adults in the U.S. own a smartphone, that's a lot of people who are at risk. A surprising 34 percent of smartphone owners do nothing to secure their mobile device, not even setting a basic code to lock the screen, according to *Consumer Reports*. College football player Laremy Tunsil recently learned how costly hacking could be, when someone stole a video off his phone that showed Tunsil inhaling marijuana through a gas mask—an embarrassment that led 12 NFL teams to bypass him in the draft, costing him millions.

What's contributing to the increase?

There are two major factors. First, more people are using their smartphones for work—especially outside the office, without thinking of the risks that come with being in a public space. Second, more people are conducting monetary transactions through their phones. Millennials in particular are comfortable doing financial business online; 94 percent of consumers under 35 access banking services through the web and mobile apps. All that financial activity on smartphones will inevitably draw the interest of hackers. "Criminals will go where the money is," Al Pascual, a fraud and security expert, told *USA Today*.

What are some schemes to be aware of?

Fake Wi-Fi networks are common lures. Hackers will set them up at a coffee shop, hotel, or other place that typically offers Wi-Fi—a practice called spoofing. The name of the network sounds legitimate, but when a user signs in, it gives the hacker direct access to his or her smartphone's contents. Mobile malware is another tactic. Malware can be hidden in fake apps—of the 10.8 million apps analyzed by Symantec in 2015, 3.3 million were identified as malicious—as well as in links in email and texts that purport to be from legitimate companies or people. This software can then breach systems, capture keystrokes, or collect data. Sometimes, though, hackers can pull off a scheme without involving you at all, a recent *60 Minutes* report showed. With no more information than a phone number, they can listen in on your calls, track your location, and even spy on you using the phone's camera.

Don't passwords help?

Locking your phone with a passcode is a must. So is using passwords that are not easy to guess. Even if they lock their phones, many people unwisely enable the devices to remember passwords to their apps so they can be easily opened, which means those accounts are accessible to anyone who hacks into the phone. Some apps and services offer a multifactor authentication system—a good option if it's available. These systems require a password to sign into an account, after which they send a one-time code, often via text message, that also has to be input. Biometric identification, such as a fingerprint, ear, or iris scan, is another security option that's gaining in popularity. But experts are cautious about the technology. Biometrics relies on physical features that determined criminals can observe and copy, warns Alvaro Bedoya, professor of law at Georgetown University. "I do know what your ear looks like, if I meet you, and I can take a high-resolution photo of it from afar," says Bedoya. "I know what your fingerprint looks like if we have a drink and you leave your fingerprints on the pint glass." He prefers passwords because they're "inherently private."

HOW TO MAKE YOUR PHONE SECURE

To foil hackers, get into good habits. Always keep your mobile operating system and apps up to date by downloading updates. The tweaked software often fixes vulnerabilities that hackers have learned how to exploit. In addition, download apps only from trusted sources; you can check developer information and user ratings on the download page. Avoid transactions on public Wi-Fi, and when you do shop or conduct other business online, make sure it's on sites that have URLs with "https" instead of "http." The former is a type of encryption—the "s" means "secure"—that keeps any data that you enter on that website safe (a lock icon in your browser's address bar is also indicative of security). Don't send personal information such as your Social Security number or credit card details in a text or email, or click on links in unsolicited emails and texts. Use encrypted messaging systems for communication, such as Apple's iMessage, Facebook Messenger, and WhatsApp. Install a "find your phone tool" in case your phone is lost or stolen; some will let you lock and wipe your phone if necessary.

AP