

# IN TODAY'S MOBILE WORLD, SECURITY NEVER GETS A BREAK

Maybe you're heading down to the cafeteria for a quick lunch, or heading out on a much needed vacation. One thing is likely—you'll probably bring your phone with you. Whether you're surfing the web or posting food pics on social media, the threat of identity theft never really goes away.

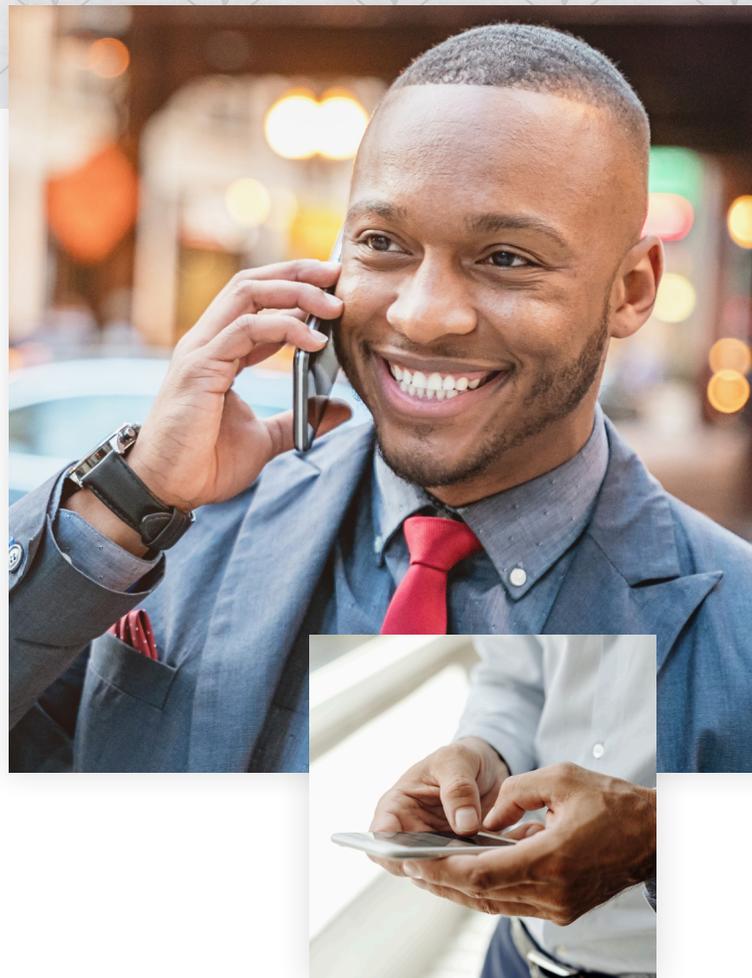
And that means your security can't take a break either. With the everyday use of mobile devices, the risk of susceptibility to hacking—and the availability of products that protect against it—have been on the rise.

## THE IMPORTANCE OF IDENTITY PROTECTION FOR YOUR DEVICES

It may seem like protecting personal information is getting almost as much attention as protecting your vehicle, home or other belongings. Staying aware of the ever-changing attempts by hackers to steal personal information is pertinent for consumers and companies alike.

Safeguarding our identities, whether from credit card skimmers, social security number theft or banking ID breaches, means that we need to keep up with evolving protection as it is delivered.

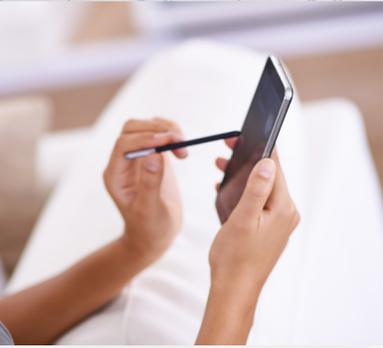
Sharing the same Wi-Fi with strangers in a coffee shop is one scenario that brings up a good example. There you are doing a bit of smartphone browsing and enjoying a beverage while a nearby culprit is accessing your privacy. Malicious apps can be found in several different categories, and gaming apps have been regular targets.<sup>1</sup>



## HAVE I BEEN HACKED?

Knowing what to look for could help you identify a hacker attack before it's too late. Common signs include:

- **Websites look different:** In some attacks, websites suddenly change their appearance.
- **Strange apps appear:** Notice an app that you don't remember installing? You could be hacked.
- **Sudden changes occur:** Malware can cause sudden changes or even serious trouble, ranging from your battery power suddenly decreasing, to apps taking control of your mobile device.
- **Unexplained online activity:** You might notice new accounts or credit charges that you didn't initiate.<sup>2</sup>



## HOW CAN I PROTECT MY IDENTITY AND DEVICES?

It's easy to think, "That won't happen to my cell phone." Yet with the variety of ways to get hacked in the spaces you might visit each day, it's not a bad idea to be extra cautious about mobile device protection.<sup>3</sup>

- Steer clear of jailbreaking (reconfiguring your devices from manufacturer standards)
- Consider a password manager to create secured and harder-to-hack login credentials
- Install security apps—read app reviews, and avoid apps with a low number of downloads<sup>3</sup>

"The biggest cybersecurity threat to mobile devices is keeping the operating system up to date with all the latest security patches and upgrades installed," says Dr. James Karagiannes, Professor of Engineering & Information Sciences at DeVry University.

Whether you are looking for protective scanning, filtering, blocking or optimization, there's a good chance you'll be able to find a product designed for your needs. Here are some additional steps that you can take<sup>3</sup>:

- Patch security and protect devices by running updates
- Freeze credit to prevent the unauthorized opening of cards and loans
- Utilize privacy settings on devices to minimize risk<sup>3</sup>

<sup>1</sup> Accessed on the internet, 3.6.2019: <http://fortune.com/2018/11/26/google-play-malware-apps/>

<sup>2</sup> Accessed on the internet, 3.6.2019: <https://www.usatoday.com/story/tech/columnist/komando/2018/05/04/has-your-computer-phone-been-hacked-heres-how-tell/559136002/>

<sup>3</sup> Accessed on the internet, 3.6.2019: <https://www.consumerreports.org/privacy/ways-to-protect-digital-privacy/>

## WHAT DO I DO NEXT?

Should you find yourself a victim of a data breach:

1. Changing your password immediately could safeguard you from future hacking attempts
2. De-authorizing social media permission settings can prevent access to your location
3. Deleting private data from the hacked account can hinder further identity theft
4. Turning on two-factor authentication<sup>3</sup> can add more security walls/checkpoints

## AM I CURRENT ON MY PROTECTION NEEDS?

So how do you stay current when it comes to cybersecurity? Here are some ideas:

- Look for blogs, books or magazines on the topic—tech is always changing
- Ask if your employer offers technical training, especially on software that you use at work
- Browse your library or police department for presentations on identity protection

Through the education partnership between your company and DeVry University, you have access to education benefits in support of your professional and life goals. To learn about transferring credits, tuition rate savings and other benefits available to you through your employer, contact your HR Representative.

