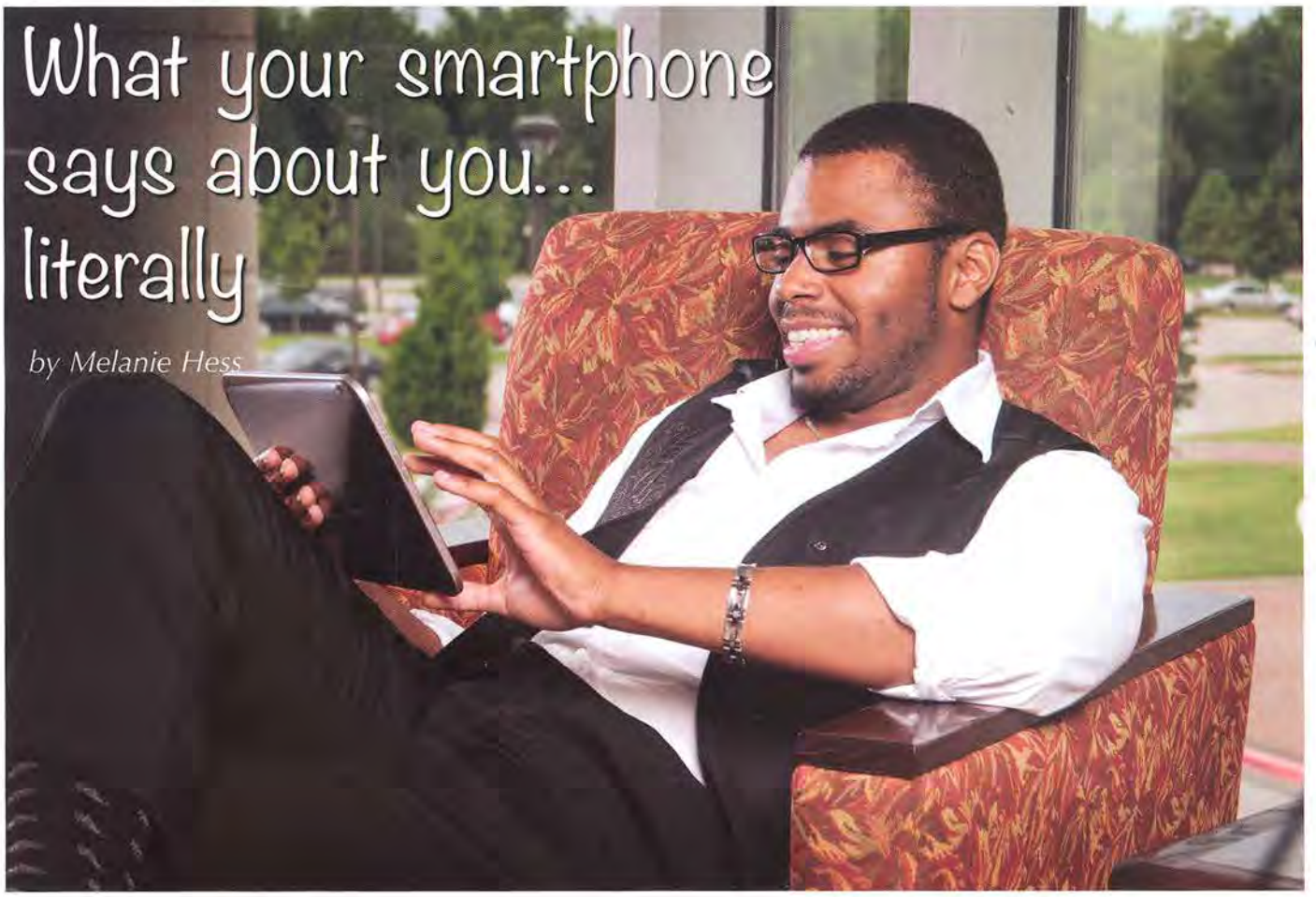
What your smartphone says about you... literally

by Melanie Hess



A neighborhood coffee shop's sign may declare "Wi-Fi is free," but in a matter of minutes "free" could cost you your email and social media accounts, credit card number, banking passwords, health records and other personal information. Those who've fallen victim to identity theft as a result of the exponentially growing mobile-device market would likely argue convenience comes with more than a monetary price.

Steve Willis, Collin College cybersecurity faculty, explained security today requires much more complexity than it did before the Internet revolution.

"Back then, no one thought about security because everyone had to go to the computer in order to use it," Willis said. "Data was confined to a few thousand tightly supervised mainframe computers worldwide. Now, it's diffused across hundreds of millions of devices that are essentially minicomputers."

Research by the International Data Corporation supports Willis' claim, as it estimates U.S. residents will own 222.4 million smartphones by 2017, with 79 percent of current users keeping their device in arms reach for all but two hours of their waking day.

College students Heather Bursik and Jacque Bussey say they fall within that 79 percent, constantly using their smartphones and mobile devices to surf the Web, watch TV, text, Skype or listen to music.

Wireless Hotspots

According to a 2013 Pew Research study, 63 percent of smartphone owners use the Internet on their phone, with 34 percent of those people claiming a cellphone functions as their primary Internet pathway.

With an ever-growing amount of data points, protecting sensitive information is vital. Unfortunately, as Willis notes, a limited portion of the general population fully understands the dangers presented by mobile technology.

"Rule of thumb, any security system that relies on millions of people to do the right thing is not a security system," Willis said.

He explains that companies like Starbucks have no incentive to secure their wireless connections when their goal is access for all.

"When you go into Starbucks and wirelessly connect, you're potentially downloading every virus known to man, and a few that aren't, onto your mobile device," Willis said.

As an individual takes that corrupted mobile device and syncs it to their company computer, the security threat becomes even greater, especially for people who hold

positions at companies like one of the major defense contractors with offices in the Dallas-Forth Worth Metroplex.

"As a known employee, you walk through the front door of the building and are walking past 90 percent of their IT security," Willis said. "You go to your desk, sit down, sync the device to your desktop calendar and have now infected the network from the inside."

For the majority of U.S. residents who don't work directly with the government, compromised cybersecurity still wreaks havoc.

Apps

Willis describes a mortgage calculator application one might download when purchasing a home. It asks the user to enter information about their income, debt, savings, taxes, interest rate and down payment. In the end, the app produces a number and does what was promised.

"However, it's also dropped a key logger—a program that records every keystroke you make on your device—so when you log into your bank or your brokerage company, that will go directly to the person who owns the key logger on your machine," Willis said. "If they have that personal information, they can change your credit card passwords, empty out your accounts, sell your stocks and take all your money."

One way Willis suggests similar apps can be avoided is through a complete review of the app's information before downloading. He encourages users to confirm the app is from a reputable company and location.

Phishing

Like a traditional desktop computer, phishing scams, fake websites that impersonate a company or organization with the goal of gaining passwords or login information, can occur on mobile devices.

Willis never recommends connecting to a public Wi-Fi hotspot for banking transactions.

However, banking from a mobile device via a secure home connection is not too much different from a desktop computer.

To prevent phishing, banks pull questions and images from completely different systems. If the image or phrases do not match the ones a user chose when setting up the account, the user will know the website is fake.

Teenagers

Taking solace in the fact that companies keeping record of financial information tend to have more secure systems, Willis does warn against one population who may not even realize they are compromising someone else's private information—teenagers.

"Think about it. How many teenagers do you see running around with mobile devices? Do you think they're thinking about security? No," Willis said. "They want to connect to whatever they want to do, whether or not it is secure."

Those same teenagers go home

and sync up to a family computer where their parents may keep personal or work-related banking, healthcare or legal information.

Willis suggests the following tips for keeping mobile devices safe:

- Don't hook up to public networks, and if you do, don't transmit any private information
- Always have anti-malware turned on and scan for viruses regularly
- Keep your operating system patches updated

"The bad guys know unpatched systems are vulnerable," Willis said. "If you don't patch them right away, you might as well put a sign on your back that says 'kick me.'"

Reaction from the Next Generation

Bursik and Bussey expressed conflicting opinions and responses about the lack of security related to mobile devices.

Bursik, who studies business marketing, believes it is the owner's responsibility to protect their device.

"If anything I'd blame the user," Bursik said. "It's the user's fault for not being careful. I avoid connecting to public wireless, and most apps are free. If someone's not taking care of their phone, that's their fault."

She concedes she believes individuals who simply don't know about the security risks aren't as at fault, but feels most people are at some level aware and just don't take the threat seriously.

As a former identity theft victim, Bursik said she takes extra steps to make sure her devices are secure.

"I have anti-virus on my computers, and on my phone I have this app called Lookout," Bursik said. "If my phone ever gets stolen, I can go onto their site, and it will take a picture of whoever has my phone without their knowledge and email it to me. Then it will GPS my phone and start signaling like a police siren."

She knows it works because it's also become a means for finding her lost phone at home.

Bussey, a civil engineering student, admits that although he feels a bit nervous transferring funds via a wireless hotspot, like many smartphone owners, it is something he has done before. After listening to Willis' expertise, Bussey said he certainly has a lot to think about.

"I think given this, people should definitely utilize their own secure connections if they're going to do something personal," Bussey said. "They should only use the other places only for watching videos or anything not too personal."

Differing from Bursik, Bussey believes network providers should exhibit more responsibility for the protection of users and be more upfront about risks, not merely noting them in fine print.

"Regardless, it's all kind of scary," Bussey said. "I'll definitely think twice before I download apps or connect to free Wi-Fi." ❖

Melanie Hess is a public relations associate at Collin College.

Photo: Nick Young, Collin College.