2

GOOGLE HACKING AND SOCIAL MEDIA SELF-DEFENSE

The first step in most hacking is *reconnaissance*, or *recon* (pronounced "REE-kon"), a military term for surveying enemy territory or observing a target. Both attackers and ethical hackers perform recon and gather information about companies, networks, and individuals using regular search engines (like Google) and specialized tools. Then, they use the information to plan the next stage of a hack.

In this chapter, you'll use Google to find information about yourself and then look for usernames and passwords with *Google hacking*. Afterward, you'll learn how to protect yourself by limiting how much information you share on social media. Information you don't share is information an attacker can't use!

Posting information about your school, sports/clubs, or weekend activities gives away your location and interests to potential attackers. An attacker who's trying to get into your account will try to guess or reset your password using personal information they find online, like a pet's name, your birthday, or your favorite restaurant. Worse yet, if you post vacation photos while you're still away from home, anyone with access to your posts could figure out your home might be empty and therefore less risky to break into.

Even sharing a picture of your cat or dog can be dangerous, because the image file itself can give away your location, as you'll see in the next section.

Location Data—Social Media's Unspoken Danger

Location data is automatically stored in most images taken with your smartphone, tablet, and many newer digital cameras. *Location data* usually means the *global positioning system (GPS)* coordinates—the precise latitude and longitude of your phone or device's location on Earth. Depending on the social media service you're using (and your settings), you may be constantly streaming your location in every picture you post. A cute picture of your cat or dog taken at home with your smartphone can give away the exact location where you live.

To view location data and other information hidden in pictures, we'll use Jeffrey's Image Metadata Viewer (*http://exif.regex.info/*). You can upload a picture file or enter the URL of a picture online to find out if there's any location data or other information in the image file.

First, go to *https://www.nostarch.com/hackingforkids/* and download *BrysonPayne-TEDx.jpg*, a picture of me taken a few years ago at a TEDx talk on coding and cybersecurity for kids. Then, go to *http://exif.regex.info/*, click **Choose file** to select the image file, check the reCAPTCHA box to confirm you're not a robot, and then click **View Image Data**. Figure 2-7 shows the hidden data (called *image metadata*).

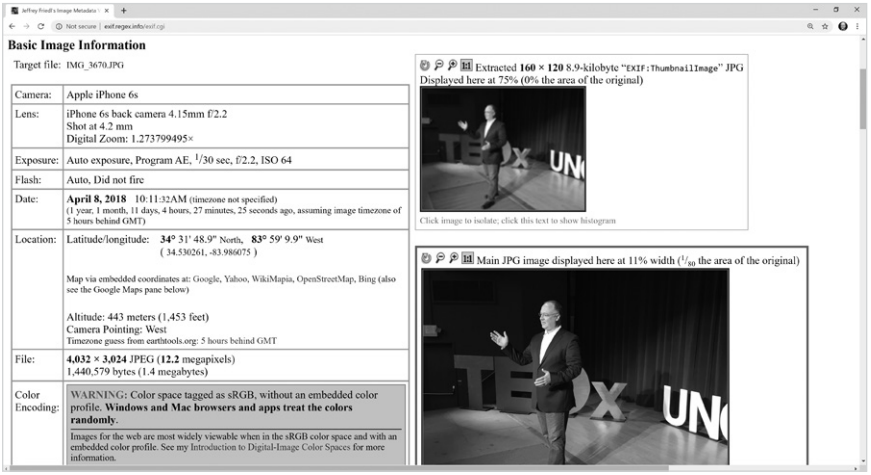

Figure 2-7: Image metadata reveals when, where, and even with which phone the photo was taken!

The picture was taken on April 8, 2018, at latitude and longitude 34.530261N, 83.986075W—the exact GPS coordinates of the auditorium where I gave the talk! The stage is located at an altitude of 443 meters (1,453 feet) above sea level, and the photo was taken on an old iPhone 6S. All of that information, and more, is hidden inside every picture you ever snap with a smartphone by default, so be careful where and how you share your photos.

Some social media apps intentionally post where you are by default—if you've ever seen someone "check in" at a cool location, that's an example. But many of the other apps on your smartphone, from map apps to email and search engines, may also be tracking your location. It's a good idea to check the security and/or privacy settings for all of the apps that you use regularly to see if you can turn off location services or use them only when needed.

Protecting Yourself on Social Media

A little more caution is likely to protect you from sharing too much online. You also need to educate your parents and relatives, friends, coaches—anyone who might take a picture of you in a group and post it to social media or say where you are at a specific time. Everyone needs to understand the importance of keeping a little more privacy in today's hyperconnected world.

Here are some of the steps you can take to protect yourself and those you care about from the dangers of social media oversharing:

Think before you share. Before posting a picture or comment, pause to think about whether you need to share it right now (or at all). At least wait until you're back home to brag about your amazing vacation.

Change your default settings. Most social media apps are set by default to share way too much information with way too many people. Go into the security or privacy settings for the app or website and turn off location data (or location services), along with any other sensitive info you don't want to share.

Limit who can see your posts. If a photo or comment gives out too much information about your daily activities, hobbies, or common places you hang out, share it privately with just the friends who'd enjoy the post.

Report cyberstalking and cyberbullying. If you ever feel threatened or harassed online or in the real world, tell a parent, teacher, or even the police. If you or someone you care about is being hurt or intimidated, find an adult you trust who can help.

Social media is a powerful connector, but it's also a powerful tool for recon and information gathering used by both black hat and white hat hackers. Don't overshare. Instead, be aware of your security and privacy settings, use social media wisely, and if anyone uses social media against you, let someone in authority know.

The Takeaway

In this chapter, you learned about free, online tools, like search engines and image metadata viewers, that hackers use to gather information about you and the people you care about. Advanced search operators can be used to pinpoint specific usernames and passwords at your school or your parents' workplace. Image metadata viewers reveal sensitive information hidden inside pictures posted online, including the exact GPS coordinates of the location where the picture was taken and what kind of smartphone was used.

You learned the importance of thinking before you share, being aware of your security and privacy settings, limiting who can see your posts, and reporting cyberbullies and cyberstalkers to the proper authorities. As smart cyberdefenders, we have to balance convenience with security to protect ourselves and the people and organizations we care about.

Each tool and technique discussed in this chapter can be used by ethical hackers to improve security and train people to protect themselves. But it can also be used by attackers to target victims. The first step in being prepared is being aware of what information is already out there. Take control of what information you share online, and you'll already be one step ahead of online attackers.

In the next chapter, you'll learn how to hack into a computer even when you've forgotten the login username and password entirely. You'll also learn how to protect a computer from physical hacking.