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!

Google Yourself (Before Your Enemy Does)

An attacker can use public information for a *phishing* attack, where they pretend to be someone you know and send a fake email asking for personal information like your password. Many company websites have a staff listing or employee directory with all the names and email addresses an attacker would need to launch a complete phishing attack, or worse.

To protect yourself, you need to find out what an attacker could see about you. Open a web browser and search for your own name or the name of a business you'd like to protect. I searched for my own name in Google, as shown in Figure 2-1.

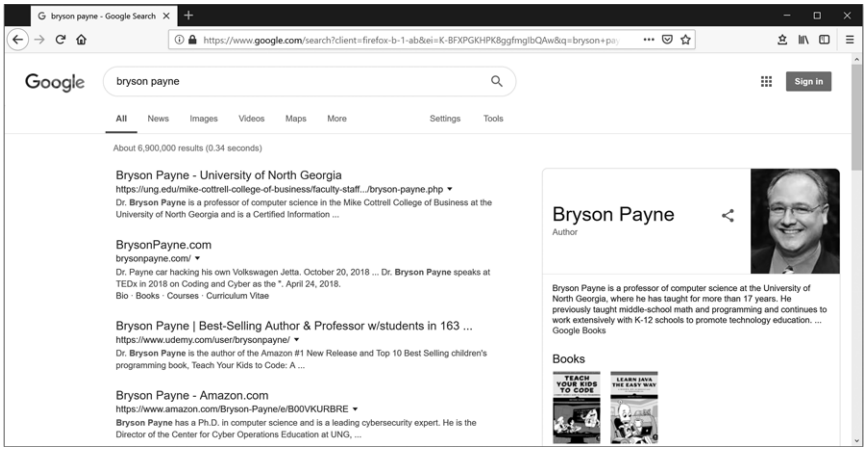

Figure 2-1: Search your own name in your favorite search engine.

Anyone on the internet can find out what I do, where I work, and that I've written books and published online courses in coding and cybersecurity. Clicking the result links turns up a lot more information, including the kind of car I drove in 2018 and some of my email addresses.

You may appear in photos from school events, news articles, sports teams, church groups, and social media pages and posts. Your name or image might even appear in articles about your family or where your parents work—things you didn't realize were on the internet.

A simple web search is good recon, but the real power of Google—Google hacking—comes from advanced search commands. With advanced searches, you can find usernames, passwords, security camera feeds, and malware. To protect yourself from malware, you need multiple defenses.

Protecting Yourself from Malware

First, make sure your computer has antivirus software installed, in case any malware gets on your computer during your research.

To avoid getting malware in the first place, you need to check if links have been infected with viruses by malicious hackers. VirusTotal is a free, online tool that scans web pages, files, and links for malware *before* you click them! You'll use VirusTotal in the next section to scan a file of passwords before you open it.

NOTE *It's safest to conduct research inside a* virtual machine (VM)*, a program that acts like another computer inside your computer. Actions you perform in a VM don't affect your computer, so the VM provides an extra layer of security. Even in a VM, you should check files in VirusTotal or another scanner before opening them, but if you open an infected file, you can simply delete and reinstall the VM. In Chapters 4 and 5, you'll build virtual machines to use for your research.*

Advanced Google Searching

You've used search engines for conducting research, writing reports, finding movie showtimes, and much more. But did you know you can use the same search engines to find vulnerable servers, unprotected devices like security cameras, usernames of important people, and even passwords?

To find usernames and passwords like an attacker would, we'll use Google *search operators*, which are symbols or words that make your search results more precise. For example, putting quotation marks (" ") around a phrase searches for the exact phrase, instead of individual words in the phrase. Using the operators *AND* and *OR* can help you find pages with both words (*3D* AND *printer*) or either word (*coding* OR *cyber*).

The operator *ext:* searches for specific *file extensions*, the filename endings for different types of files, like *docx* for Microsoft Word documents, *txt* for plaintext, *pdf* for PDF files, *xlsx* for Microsoft Excel spreadsheets, and so on. The operator *site:* searches for results on specific sites, like site:nostarch.com, site:yourschool.edu, or site:hackingforkids.com.

Finding Usernames and Passwords with Google

Let's use the ext: search operator to find spreadsheets containing passwords. Open Google's search engine in your browser and type **ext:xls password** into the search field, as shown in Figure 2-2.

Remember *not* to click any of the results, as a skilled attacker could easily hide a virus or ransomware in an infected spreadsheet file (or make an infected web page look like a spreadsheet to the search engine). *Ransomware* is a nasty type of malware that encrypts all your files and demands that you pay a ransom to get your data back, so be careful!

You'll likely find dozens of usernames and passwords right in the search page. For example, the top result in Figure 2-2 shows 2016 US election campaign passwords allegedly stolen by hackers attempting to interfere in the US presidential election.

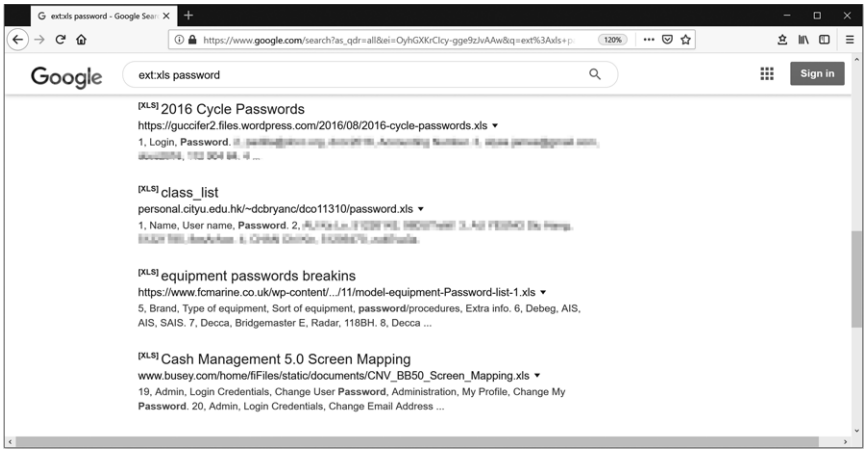

*Figure 2-2: Typing **ext:xls password** finds Excel spreadsheets filled with usernames and passwords.*

Before clicking any of the files you've found, copy the URL of the file (highlight the link address in the Google results, right-click or CONTROL-click (on a Mac), and go to **Copy link address** or **Copy link location**). Then open *https://www.virustotal.com/* in a new tab, click the **URL** tab, and paste the copied URL into the search field, as shown in Figure 2-3.

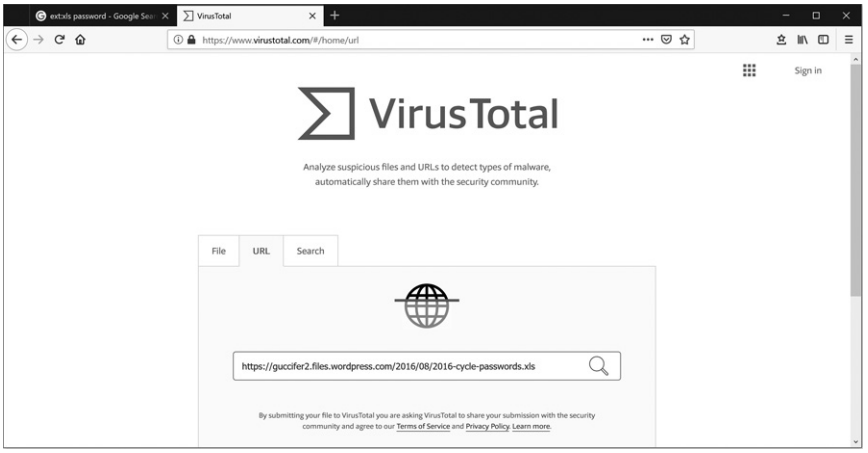

Figure 2-3: Check suspicious web links before clicking them by scanning them through VirusTotal.

Click the search icon (the magnifying glass) to scan the link. In Figure 2-4, VirusTotal has scanned the password spreadsheet file with more than 60 different antivirus engines, and none of them found any sign of infection.

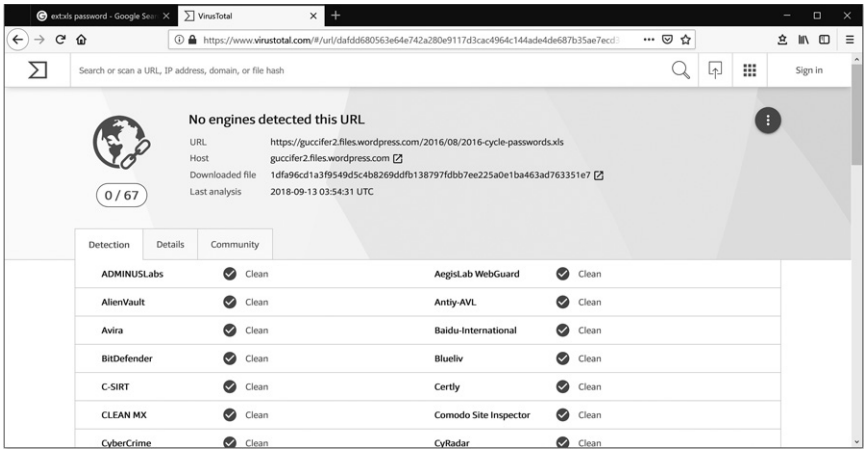

Figure 2-4: The password spreadsheet we selected appears safe to open.

WARNING *Files may contain advanced malware that doesn't show up in any normal virus scans on VirusTotal. For that reason, it's best to open questionable spreadsheet or document files from inside a virtual machine like the ones you'll create in Chapters 4 and 5. A VM can protect us even while we're doing research in a search engine!*

Try the search again, but now type **ext:txt** or **ext:pdf** to check for other file types containing passwords. To search for your own information, search for your username and the word *password* (for example, "bryson_payne AND password"). *Never type your actual password into Google or any other search engine.* If you find a password of your own, change it immediately. (If you conduct a search on behalf of a friend, family member, or teacher with their permission and find one of their passwords, let them know they need to change that password!)

Checking for Passwords at School or at Work

You can use the site: search operator to look for leaked passwords on a specific website. For example, in Figure 2-5, I've typed "site:ung.edu password" into Google to find out if any student or faculty passwords from my university, the University of North Georgia, are stored on our public web server.

As you can see, there were no text files or spreadsheets listed, but the bottom result is an old news article about the default password assigned to incoming university students. At the time that article appeared, an attacker could have used the default password information to guess thousands of students' initial passwords.

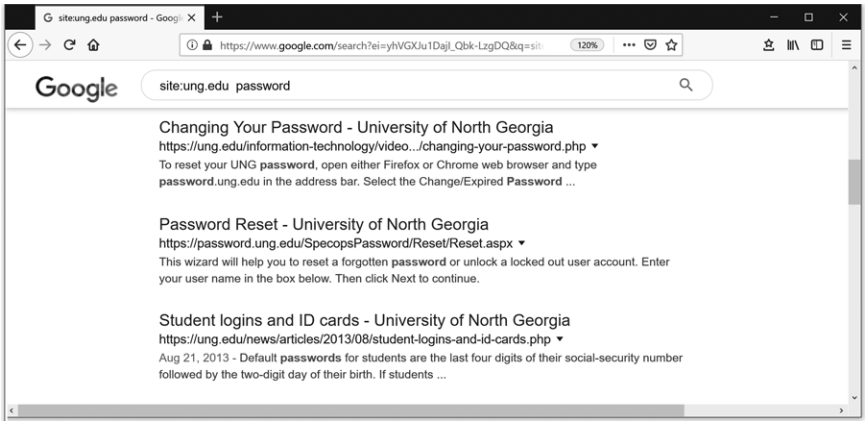

Figure 2-5: Use the site: search operator to search for results on your school's website.

WARNING

Suppose you find passwords from your school, your work, or your friends' or family's accounts. First, never try those passwords yourself—that would be as creepy and unethical as finding their keys and trying to open their front door without permission. An ethical hacker would report the potential password leak to an IT employee at school or work, and they would tell the friend or family member that their password might be exposed and that they should immediately change the password for any account that uses that password or a similar one.

You can also combine the site: operator with other operators. For example, "ext:pdf site:ung.edu bryson_payne AND password" searches for PDF files on my university's website that contain my username and the word *password*.

These are just a few of the search operators you can use in Google to find sensitive information. Over the years, other hackers have created a database of Google hacks to record useful search operator combinations.

The Google Hacking Database

The *Google Hacking Database (GHDB)* is a public listing of thousands of Google search operator combinations that can be used to find passwords, specific types of devices or equipment connected to the internet, particular web applications with vulnerabilities, and more.

GHDB was a project started by Johnny Long of Hackers for Charity; the database is now maintained by Offensive Security, the same team that supports Kali Linux and other hacking and security tools. You can find the GHDB at *https://www.exploit-db.com/google-hacking-database/* or by searching for "Google Hacking Database" in your search engine.

Go to the GHDB at *https://www.exploit-db.com/google-hacking-database/* and enter **password** in the search box, as shown in Figure 2-6. The database will display all *search queries* (combinations of operators and text to search for) that contain the word *password*.

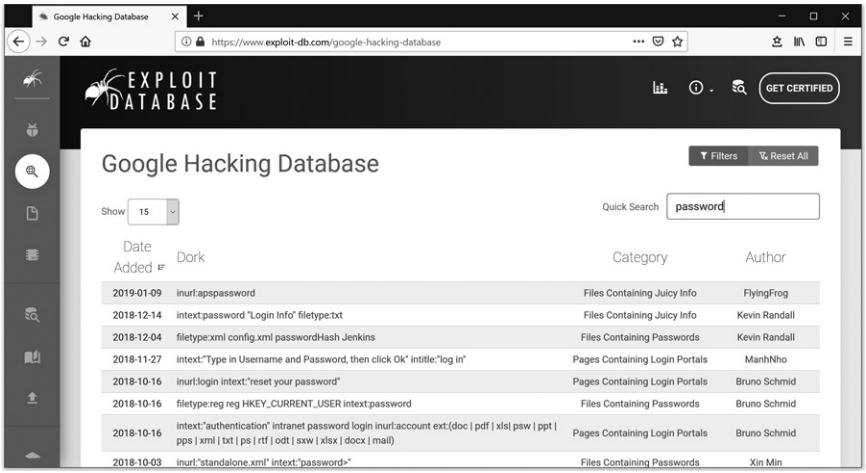

Figure 2-6: The Google Hacking Database password search queries

Clicking any of the entries in the GHDB will show information about that specific search query, and you can even go directly to Google and try the search.

WARNING *Remember to check any files or sites you find in an online scanner like VirusTotal before opening them, though.*

Just as with your family's or friends' passwords, if you find sensitive information about a local business or about your school, it's good ethical practice to let someone know the information is publicly available, so they can change their passwords or take other action as needed.

Speaking of your family and friends, let's talk about another frightening source of too much information: social media.

Social Media and the Dangers of Oversharing

You might have been surprised—even a bit scared—to find out how much information Google already has about you, your school, or your favorite company. However, you may be leaking much more specific and sensitive information every day, or several times per day, through social media.

Here's a quick exercise you can do for yourself and share with friends or family: take 5 minutes to do a quick recon mission on your favorite social media account or accounts. Can you find out where you live, what kind of pets you have (and what their names are), what your siblings' names are, or maybe even your parents' names? What about pictures from your most recent birthday? From the date of the pictures and the age mentioned (for example, if someone posted "Happy 15th Birthday!"), could an attacker figure out your exact date and year of birth? What else can you find about the places you go regularly, like sporting events, and the people you hang out with?

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*).

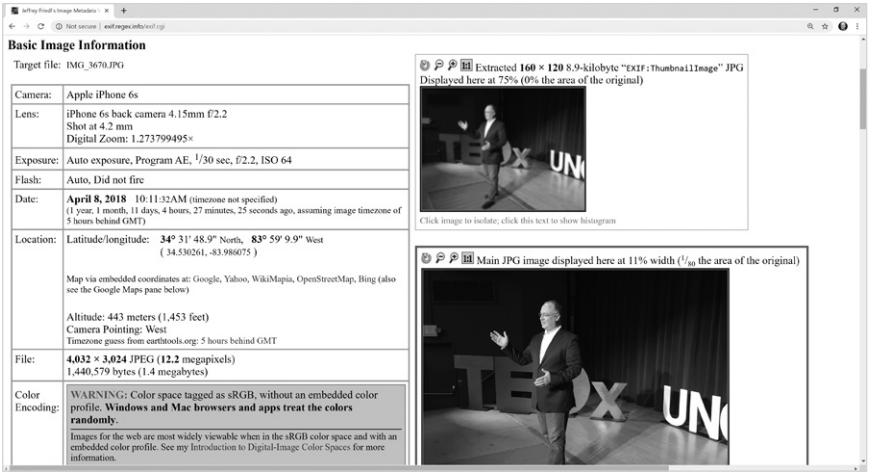

Figure 2-7: Image metadata reveals when, where, and even with which phone the photo was taken!

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.