Chapter 1

Using Digital Resources Responsibly

THE LPI SECURITY ESSENTIALS EXAM TOPICS COVERED IN THIS CHAPTER INCLUDE THE FOLLOWING:

✓ **021.1 Goals, roles and actors**

- Understanding of the importance of IT security

✓ **021.3 Ethical behavior**

- Understanding the implications for others of actions taken related to security
- Handling information about security vulnerabilities responsibly
- Handling confidential information responsibly
- Awareness of personal, financial, ecological, and social implication of errors and outages in information technology services

✓ **024.3 Network encryption and anonymity**

- Understanding of the concepts of TOR
- Awareness of the Darknet

✓ **025.2 Information confidentiality and secure communication (weight: 2)**

- Understanding the implications and risks of data leaks and intercepted communication
- Understanding of phishing and social engineering and scamming
- Understanding the concepts of email spam filters

✓ 025.3 Privacy protection

- Understanding of the importance of personal information
- Understanding of how personal information can be used for a malicious purpose
- Understanding of the concepts of information gathering, profiling, and user tracking
- Managing profile privacy settings on social media platforms and online services
- Understanding of the risk of publishing personal information
- Understanding of the rights regarding personal information (e.g., GDPR)

"With great power comes great responsibility."

Words of wisdom. That's the message displayed for administrators when they log in for the first time to many Linux distributions. Who said those words first? Aristotle? Kant? Nope. Spiderman's uncle. But hey, accept the truth from any source.

While we'll discuss protecting yourself from attack at length later in the book, this chapter is all about responsibilities. It's about your responsibilities both as a *consumer* of computer technologies and as an *administrator* of computer technologies. It's your job to make sure nothing you do online or with your devices causes harm to anyone's assets.

How is all this relevant to the world of information technology (IT) and, specifically, to IT security? Computers amplify your strengths. No matter how much you can remember, how fast you can calculate, or how many people's lives you can touch, it'll never come close to the scope of what you can do with a computing device and a network. So, given the power inherent in digital technologies and the depth of chaos such power can unleash, you *need* to understand how it can all go wrong before you set off to use it for good.

The rest of this chapter will explore the importance of considering how your actions can impact people's personal and property rights and privacy and how you can both ensure and assess the authenticity of online information.

I'm not a lawyer, and this book doesn't pretend to offer legal advice, so we're not going to discuss some of the more esoteric places where individual rights can come into conflict with events driven by technology. Instead, we'll keep it simple. People should be able to go about their business and enjoy their interactions with each other without having to worry about having physical, financial, or emotional injury imposed on them. And you should be ready to do whatever is necessary to avoid or prevent such injuries.

Protecting Personal Rights

These days, the greatest technology-based threats to an individual's personal well-being will probably exist on one or another social media platform. Facebook, Twitter, LinkedIn, and other online sites present opportunities for anyone to reach out to and communicate with millions or even billions of other users. This can make it possible to build entire businesses or social advocacy movements in ways that would have been unthinkable just a few years back. But, as we all now know, it also makes it possible to spread dangerous scams, political mischief, and social conflict.

As the man said, "With great power comes great responsibility." Therefore, you need to be conscious of the possible impact of any interaction you undertake. This will be true not only for your use of your own social media or email/messaging accounts but also for any interactions taking place on sites or platforms you administrate. You could, for instance, be held legally responsible for anonymous comments left on your blog or for the use of email accounts belonging to your organization. It can be a hard balance to achieve. Are your policies unnecessarily allowing damaging content to be published or, alternatively, unfairly restricting innocuous content?

A helpful tool for maintaining perspective in these areas is to apply the *grandmother test*. What's that? Before posting a message or comment on any online forum, take a minute to read it over one or two more times and then ask yourself, "Would both my grandmothers approve of what I've written? Is there anything that would make them uncomfortable?" In other words, ask yourself whether anyone could reasonably feel threatened or bullied by what you're about to publish. The bottom line is to make generous use of common sense and goodwill.

With typical attention to such details, the social media community has come up with new names to describe each of the nastiest online threats. You should, unfortunately, be familiar with each of them.

Cyberstalking Stalking isn't specific to online activities, but that doesn't make it any less frightening. In general terms, a stalker persistently follows and observes a target, often with the goal of forcing an unwanted reaction. In the online world, *cyberstalking* can include electronic monitoring of a target's online accounts and activities. Harassing cyberstalking can escalate beyond mere monitoring to include threats, slander, and identity theft.

Cybermobbing Mobbing involves large groups of people banding together to engage in bullying behavior. The nature of many social networking platforms—in particular the prevalence of anonymous accounts and the ease by which users can connect to each other—lends itself to mob formation. Often, all it can take is a single public post expressing an unpopular position, and the power of tens of thousands of users can be brought to bear with the goal of making life miserable for the post's author.

Doxxing Whether you present yourself to the online world using your real name or through an anonymous identity, you certainly don't want your complete personal profile to become public. Considering all the data that's already available on the Internet, it's often not hard for people with time on their hands to track down your physical address and private phone numbers. But making such information easily available on popular social media sites with the intention of causing the target harm is wrong—and, in some jurisdictions, also a crime. Victims of public doxxing have experienced relatively mild annoyances like middle-of-the-night pizza deliveries. But the practice has also proven deadly: it's been used as part of "swatting" attacks, where people call a victim's local police department claiming there's a violent crime in progress at the victim's address. More than one doxxer has been imprisoned for what, at the time, must have seemed like a clever prank.

Protecting Digital Privacy

Your primary concern must always be to secure the data under your control. But have you ever wondered why that is? What's the worst that could happen if copies of your data are stolen—after all, you'll still have the originals, right? Well, if your organization is in the business of profiting from innovations and complex, hard-to-reproduce technology stacks, then the consequences of data theft are obvious. But even if your data contains nothing more than private and personal information, there's a lot that can go wrong.

Let's explore all that by way of posing a few questions.

What Is Personal Data?

Your personal data is any information that relates to your health, employment, banking activities, close relationships, and interactions with government agencies. In most cases, you should have the legal right to expect that such information remains inaccessible to anyone without your permission.

But "personal data" could also be anything that you contributed with the reasonable expectation that it would remain private. That could include exchanges of emails and messages or recordings and transcripts of phone conversations. It should also include data—like your browser search history—saved to the storage devices used by your compute devices.

Businesses and government departments that handle many kinds of data must apply information classification systems to ensure that their data isn't mishandled. They might, therefore, label all data objects using designations like *confidential*, *classified,* and *restricted*. Clear policies based on those classifications should be enforced for the management of all that data.

Among other measures, organizations can seek to control the way their data is shared by imposing nondisclosure agreements (NDAs). Outside consultants doing work with such an organization might be required to sign an NDA that precisely defines limits for how the information they'll be shown should be handled.

You have the right to expect that social media platforms and other third-party organizations respect the privacy settings you choose for your accounts. However, it's your responsibility to ensure that your settings properly reflect your needs and preferences. You should make it a practice, from time to time, to revisit your account settings and, if necessary, update them.

Governments, citing national interest concerns, will reserve the right for their security and enforcement agencies to forcibly access your personal data where legally required. Of course, different governments will set the circumstances defining "legally required" according to their own standards. When you disagree, some jurisdictions permit legal appeal.

Where Might My Personal Data Be Hanging Out?

The short answer to that question is "probably lots of places you wouldn't approve." The long answer will begin with something like "I can tell you, but expect to become and remain deeply stressed and anxious." In other words, it won't be pretty. But since you asked, the following are some things to consider.

Browsing Histories

The digital history of the sites you've visited on your browser can take more than one form. Your browser can maintain its own log of the URLs of all the pages you've opened. Your browser's cache will hold some of the actual page elements (like graphic images) and *state* information from those websites. Online services like Google will have their own records of your history, both as part of the way they integrate your various online activities and through the functionality of website usage analyzers that might be installed in the code of the sites you visit.

Some of that data will be anonymized, making it impossible to associate with any one user, and some is, by design, traceable. A third category is *meant* to be anonymized but can, in practice, be decoded by third parties and traced back to you. Given the right (or wrong) circumstances, any of that data can be acquired by criminals and used against your interests.

E-commerce and Social Media Account Data

Everything you've ever done on an online platform—every comment you've posted, every password you've entered, every transaction you've made—is written to databases and, at some point, used for purposes you didn't anticipate. Even if there was room for doubt in the past, we now know with absolute certainty that companies in possession of massive data stores will *always* seek ways to use them to make money. In many cases, there's absolutely nothing negative or illegal about that. As an example, it can't be denied that Google has leveraged much of their data to provide us with mostly free services that greatly improve our lives and productivity.

But there are also concerning aspects to the ways our data is used. Besides the possibility that your social media or online service provider might one day go to the "dark side" and abuse their access to your data, many of them—perhaps most infamously, Facebook—have sold identifiable user data to external companies. An even more common scenario has been the outright theft of private user data from insufficiently protected servers. This is something that's already happened to countless companies over the past few years. Either way, there's very little you can do to even track, much less control, the exciting adventures your private data may be enjoying—and what other exotic destinations it might reach 1, 5, or 10 years down the road.

Government Databases

National and regional government agencies also control vast stores of data covering many levels of their citizens' behavior. We would certainly hope that such agencies would respect their own laws governing the use of personal data, but you can never be sure that government-held data will never be stolen—or shared with foreign agencies that aren't bound by the same standards. It also isn't rare for rogue government agencies or individual employees to abuse their obligations to you and your data.

Public Archives

The Internet never forgets. Consider that website you quickly threw together a decade ago as an expression of your undying loyalty to your favorite movie called...wait, what was its

name again? A year later, when you realized how silly it all looked, you deleted the whole thing. Nothing to be embarrassed about now, right? Except that there's a good chance your site content is currently being stored and publicly displayed by the Internet Archive on their Wayback Machine (`https://archive.org/web/web.php`). It's also not uncommon for online profiles you've created on social networking sites like Facebook or LinkedIn to survive in one form or another long after deletion.

The Dark Web

As we'll learn in Chapter 6, "Encrypting Your Moving Data," information can be transferred securely and anonymously through the use of a particular class of encrypted connections known as a *virtual private network* (VPN). VPNs are tools for communicating across public, insecure networks without disclosing your identifying information. That's a powerful security tool. But the very same features that make VPNs secure also give them so much value inside the foggy world of the Internet's criminal underground.

A popular way to describe places where you can engage in untraceable activities is using the phrase "dark web." The dark web is made up of content that, as a rule, can't be found using mainstream Internet search engines and can be accessed only through tools using specially configured network settings. The private or hidden networks where all this happens are collectively known as Darknet. The tools used to access this content include the Tor anonymity network that uses connections that are provided and maintained by thousands of participants. Tor users can often obscure their movement across the Internet, making their operations effectively anonymous.

Tor is actually an acronym that stands for "The Onion Router." The many layers that make up an onion are an effective way to visualize the Tor protocol. Tor-based data can be transmitted across a network in the form of browser requests, for instance. A request can be encrypted in a way that permits each network node it visits to "peel back" only a single layer of encryption, exposing just enough information to direct the data to the next step along its path. The request is only fully decrypted once it reaches its final destination.

Tor is best known for allowing for anonymous browsing sessions—something designed to protect the identity of server clients. However, server identities can be similarly protected using what's known as *hidden services* (or, more often, *onion services*). When both clients and servers are using Tor, you can achieve true end-to-end encryption. Onion servers are identified by a string of 56 characters followed by `.onion`.

Like VPNs, the dark web is often used to hide criminal activity, but it's also popular among groups of political dissidents seeking to avoid detection and journalists who communicate with whistleblowers.

A great deal of the data that's stolen from servers and private devices eventually finds its way to the dark web.

What Are My Responsibilities as a Site Administrator?

Besides the moral obligation to protect your users and organization from harm, you will probably also need to ensure that your infrastructure configurations meet legal and

regulatory requirements. One particularly prominent set of laws is the European Union's General Data Protection Regulation (GDPR). The GDPR affects any organization that processes data that's either sent to or from the European Union (EU). Failure to appropriately protect the privacy and safety of protected data moving through EU territory can result in significant—even crippling—fines.

Other regulatory systems that might, depending on where and how your organization operates, require your compliance include the Payment Card Industry Data Security Standards (PCI-DSS) administered by major international credit card companies and the U.S. government's Health Insurance Portability and Accountability Act (HIPAA).

Besides addressing your regulatory requirements, it's worthwhile thinking about the real-world consequences of failing to effectively protect your users' data. The impact of breaches, outages, and data loss events can go far beyond financial damage. It's not at all uncommon for clients and users to suffer permanent personal, social, health, or even ecological damage from IT disasters.

Can Escaped Genies Be Forced Back into Their Bottles?

Well, let me ask you this: have *you* ever successfully returned a genie to its bottle? I thought so. Unfortunately, it would probably be just as impractical to even try to find and delete all copies of stolen data that's been spread across an unknown number of sites—including some on the dark web.

Even getting private references removed from search engine results can involve a long, uphill struggle with no guarantee of success. Thanks to the GDPR, European residents can request help from Google using the Personal Information Removal Request Form. But you can never be sure how that will turn out, and sometimes submitting your request can make things worse. Considering taking down an offending website. Are you sure you even know how to find all the copies? Are you aware, for instance, that the Internet Archive project (`https://archive.org/web`), as of this writing, hosts historical versions of more than 772 billion web pages? I've actually used the project to recover lost data from 15-year-old iterations of my own sites.

What Can I Do as a User?

Here's a good place to start: think carefully before posting anything on an online platform. Are you revealing too much about yourself? Will you be comfortable having your future employers and grandchildren read this 10 or 20 years from now? Try to anticipate the places your content might end up and what value it might have for people you've never met—people unconstrained by ethical concerns who care only about making money.

Be realistic about your data. Don't assume that the contacts with whom you share files and information will be the only ones to see them. Even if your own accounts will remain secure, theirs might not. And who says those friends or colleagues will respect your privacy preferences indefinitely?

Never assume the file storage or sharing platform you're relying on won't change their privacy rules at some point in the future. Or, even better, that they'll never decide to sell your data to someone else.

Finally, here's one that makes a ton of sense and is absolutely obvious. But not only am I sure you've never done it, I'm confident that you probably never will. Remember those check boxes you're required to click before you can open a new online account? You know, the ones that say something like this:

> "I have read and accept the terms of the privacy policy."

Well, have you ever actually read through one of those documents before clicking? Me neither. I mean, Google's Privacy and Terms document (`https://policies.google.com/privacy?hl=en`) is around the same length as this chapter (and not nearly as much fun). Who's got the time? On the other hand, reading it from start to finish would probably give you important insights into the real-world consequences of using Google services. It might even convince you to change the way you use the product. And reading the privacy documents for *all* the platforms you use would undoubtedly make you a better and safer consumer.

But we all know that's not happening, right?

Establishing Authenticity

You've got a strong and active interest in distinguishing between what's real and what's fake in your digital life. Considering how much unreliable content is out there, making such distinctions might not be so simple. Many of the choices you make about your money, property, and attitudes will at least partly rely on information you encounter online, and you certainly don't want to choose badly. So, here's where we'll talk about ways you can test and validate content to avoid being a victim.

Think About the Source

Always carefully consider the source of the information you want to use. Be aware that businesses—both legitimate and not—will often populate web pages with content designed to channel readers toward a transaction of some kind. The kind of page content that'll inspire the most transactions is not necessarily the same as content that will provide honest and accurate information. That's not to say that private business websites are always inaccurate—or that nonprofit organizations always produce reliable content—but that you should take the source into account.

With that in mind, I suggest you're more likely (although by no means guarantied) to get accurate and helpful health information, for example, from the website of a well-known government agency like the UK's Department of Health and Social Care or an academic health provider like the Mayo Clinic (`www.mayoclinic.org`) than from a site called `CheapCureZone.com` (a fictitious name, but representative of hundreds of real sites).

Similarly, you should consider the context of information you're consuming. Did it come in an email message from someone you know? Were you expecting the email? Did you get to a particular web page based on a link in a different site? Do you trust that site?

By the way, I personally consider Wikipedia to be a largely accurate and reliable information site that generally includes useful links to source material. Biased or flat-out wrong information will sometimes turn up on pages but, besides for pages covering politically controversial topics, it's rare. More often than not, problematic pages will contain warnings indicating that the content in its current state is being contested. And if you do find errors? Fix 'em yourself.

Be Aware of Common Threat Categories

Spam—unsolicited messages sent to your email address or phone—is a major problem. Besides the fact that the billions of spam messages transmitted daily consume a fortune in network bandwidth, they also carry thousands of varieties of dangerous malware and just plain waste our time.

Your first line of defense against spam is to make sure your email service's spam filter is active. A spam filter will scan all incoming emails for content and language that suggests it's not something you would normally want to read. Good filters will pay particular attention to dangerous file attachments and links to dangerous Internet sites. When a message is categorized as spam, most filters will move the message to a special spam folder, where you could examine it for yourself or just delete it. Occasionally, a false positive will inadvertently send an important email to the spam folder. So, you should take a look every now and then.

Your next step: educate yourself about the ways spammers use *social engineering* as part of their strategy.

Spoofing involves email messages that misrepresent the sender's address and identity. You probably wouldn't respond to an email from `suspiciousguy@darkw3b.com`, but if he presented himself as `e.musk@tesla.com`, you might reconsider. At the very least, recognize that email and web addresses can be faked. Organizations using DomainKeys Identified Mail (DKIM) to confirm the actual source of each email message can be effective in the fight against spoofing.

Phishing attacks—which are often packaged with spoofed emails—involve criminals claiming to represent legitimate organizations like banks. A phishing email might contain a link to a website that looks like it belongs to, perhaps, your bank but doesn't. When you enter your credentials to log in, those credentials are captured by the website backend and then used to authenticate to the actual banking or service site using your identity. I don't have to tell you how that can end.

Always carefully read the actual web address you're following before clicking—or at the very least, before providing authentication details. Spelling counts: `gmall.com` is *not* the same as `gmail.com`. Consider using multifactor authentication (MFA) for all your account logins. That way, besides protecting you from the unauthorized use of your passwords, you should ideally notice when you're not prompted for the secondary authentication method and back away.

In general, be deeply suspicious of desperate requests for help and unsolicited job offers. Scammers often pretend to be relatives or close friends who have gotten into trouble while traveling and require a quick wire transfer. Job offers can sometimes mask attempts to access your bank account or launder fake checks written against legitimate businesses.

It's a nasty and dangerous world out there. Think carefully. Ask questions. Seek a second opinion. Always remember the wise rule: "If it's too good to be true, it probably isn't." And remember, the widow of Nigeria's former defense minister does *not* want you to keep $34 million safe for her in your bank account. Really.

Summary

You are responsible for digital interactions and operations taking place using your accounts or on accounts administrated by you. You should work to prevent harm from resulting from any of that activity.

Understanding how criminals—and careless administrators—can put your data at risk is critical to learning how to protect yourself and the users you're responsible for.

Before engaging in online activity, always try to think through the possible short- and long-term consequences. Is what you're about to do likely to cause you or others harm?

Reading the privacy policy documents associated with the platforms and services you use can help you understand the threat environment you'll be using.

Always examine the context of online information: is it part of a reliable website or associated with a well-known institution?

Be aware of the kinds of threats you're likely to face as you go about your life on the Internet. Only by understanding what can go wrong can you hope to protect yourself and the people who rely on you.

Exam Essentials

Understand common online attack behaviors, including cyberstalking, cybermobbing, and doxxing. Cyberstalking involves persistently pursuing an individual's online and private identity in a threatening way. Cybermobbing is the cooperation of the owners of large numbers of online social media accounts to harass an individual with whom they don't agree. Doxxers research and then publicize private information about an individual they want to harm.

Understand the kinds of personal data that are the most sensitive and vulnerable to abuse. Your browser history, social media account activities, online e-commerce transaction information, and health records are all categories of personal data that require special attention and protection.

Understand the regulatory requirements for which you and your infrastructure are responsible. Businesses operating in the European Union must conform to the policies of the General Data Protection Regulation (GDPR). The Payment Card Industry Data Security Standards (PCI-DSS) and the U.S. government's Health Insurance Portability and Accountability Act (HIPAA) are also important standards.

Be familiar with common kinds of digital "social engineering" attacks. Spam describes unsolicited email messages sent with the goal of getting you to respond, usually by purchasing a product of doubtful value. Spoofing misrepresents the origin and sender of the email. Phishing attacks try to get you to interact with a web resource that's made to look like an actual legitimate site.

Review Questions

1. What best describes doxxing?
   - **A.** Falsely and illegally directing law enforcement authorities toward a nonexistent crime
   - **B.** Publicizing a target's personal contact and location information without authorization
   - **C.** Persistent and unwanted monitoring and harassing of a target
   - **D.** A coordinated social media–based attack against an individual involving large numbers of attackers
2. What best describes cybermobbing?
   - **A.** Publicizing a target's personal contact and location information without authorization
   - **B.** Falsely and illegally directing law enforcement authorities toward a nonexistent crime
   - **C.** A coordinated social media–based attack against an individual involving large numbers of attackers
   - **D.** Persistent and unwanted monitoring and harassing of a target
3. As an employer, which of the following are most likely to present legal liabilities for you and your organization? (Choose two.)
   - **A.** Threatening comments posted by your employees on your organization's website
   - **B.** Threatening comments posted by your employees on their own social media accounts
   - **C.** Criminal activity (like cyberstalking) launched by an employee using public resources
   - **D.** Criminal activity (like cyberstalking) launched using your organization's website resources (like a technical support forum)
4. Which of the following types of data should generally be considered personal and private? (Choose two.)
   - **A.** The browser history on a user's personal computer
   - **B.** Old social media posts
   - **C.** A consumer's purchasing history with an online store
   - **D.** Official records of criminal trial proceedings
5. What elements are likely to be included in your "browser history"? (Choose two.)
   - **A.** Transcripts of recent text message conversations
   - **B.** Passwords you've used for online application authentication
   - **C.** Information about your computer and software profile
   - **D.** Information about the state of a past website session

6. Why should you be conscious and concerned about any of your personal data that the owners of online services and applications might control? (Choose two.)

- **A.** Because you could be prevented from accessing such information on your own
- **B.** Because it might be stolen by third parties and mined for information that might prove damaging to you
- **C.** Because it might be sold to third parties or used by the services themselves in ways that infringe on your rights
- **D.** Because your information might change and updating remote databases can be time consuming and inconvenient

7. What best describes the General Data Protection Regulation (GDPR)?

- **A.** It mandates the destruction of financial and health data as soon as an organization is no longer required to retain it.
- **B.** It mandates the retention of financial and civil records related to European Union government activities.
- **C.** It mandates the protection, privacy, and safety of healthcare-related data in the United States.
- **D.** It mandates the protection, privacy, and safety of personal data moving through EU territories.

8. Which of these is an industry (rather than government-mandated) regulatory framework?

- **A.** HIPAA
- **B.** PCI-DSS
- **C.** GDPR
- **D.** Sarbanes-Oxley (SOX)

9. Why is it important to read an organization's privacy policy if you intend to interact with their service? (Choose two.)

- **A.** To better understand the security and privacy safeguards built into the application
- **B.** To be better able to predict the chances the organization might misuse or unnecessarily expose your data
- **C.** To better understand the true potential costs of using the service in question
- **D.** To understand how the organization might use your data

10. What best describes spoofing?

- **A.** Using an Internet address (URL) that closely resembles a well-known, legitimate site
- **B.** Misrepresenting the origin address within an email message
- **C.** Attempting to trick individuals into revealing private information
- **D.** Sending unsolicited and often dishonest email messages

11. What best describes phishing?

- **A.** Using an Internet address (URL) that closely resembles a well-known, legitimate site
- **B.** Sending unsolicited and often dishonest email messages
- **C.** Attempting to trick individuals into revealing private information
- **D.** Misrepresenting the origin address within an email message

12. What should you consider when assessing the value of online information you encounter? (Choose two.)

- **A.** The reputation of the source
- **B.** Whether the information can be verified by third-party sources
- **C.** The number of outbound links associated with the source
- **D.** The presence of proper website encryption