Part 5

Handling a Security Incident (This Is a When, Not an If)

IN THIS PART …

Recognize signs that you may have suffered a security breach.

Understand when you may be impacted from someone else's security breach.

Recover from hacked email, social media accounts, computers, and networks.

Recover from ransomware and other forms of malware.

Find out what to do if your computer or mobile device is stolen.

Chapter 11

Identifying a Security Breach

IN THIS CHAPTER

- **Understanding why it's critical to know if you were breached**
- **Identifying overt and covert breaches**
- **Recognizing various symptoms of covert breaches**

Despite valiant efforts to protect your computer systems and data, you may suffer some sort of breach. In fact, the odds that your data will — at some point — be breached are close to 100 percent. The only real question is whether the breach will take place on your system or on someone else's.

Because you're ultimately responsible for maintaining your own computer systems, you need to be able to recognize the signs of a potential breach of your equipment. If a hacker does manage to penetrate your systems, you need to terminate his or her access as quickly as possible. If your data has been manipulated or destroyed, you need to restore an accurate copy. If systems are malfunctioning, you need to get them back on track.

In this chapter, you discover the symptoms of a breach. Armed with this knowledge, you can hopefully recognize if something is amiss and know the corrective actions to take.

If you've already receive notification from a third-party-provider where you store data that your data has been compromised or may have been compromised, refer to Chapter 13.

Identifying Overt Breaches

The easiest breaches to identify are those in which the attacker announces to you that you've been breached and provides proof of that accomplishment.

Three of the most common overt breaches are those involving ransomware, defacement, and claimed destruction.

Ransomware

Ransomware is a form of malware that encrypts or steals data on a user's device and demands a ransom in order to restore the data to the user's control (see Figure 11-1). Typically, ransomware includes an expiration date with a warning to the tune of "pay within *x* hours or the data will be destroyed forever!" (See Chapter 2 for more on ransomware.)

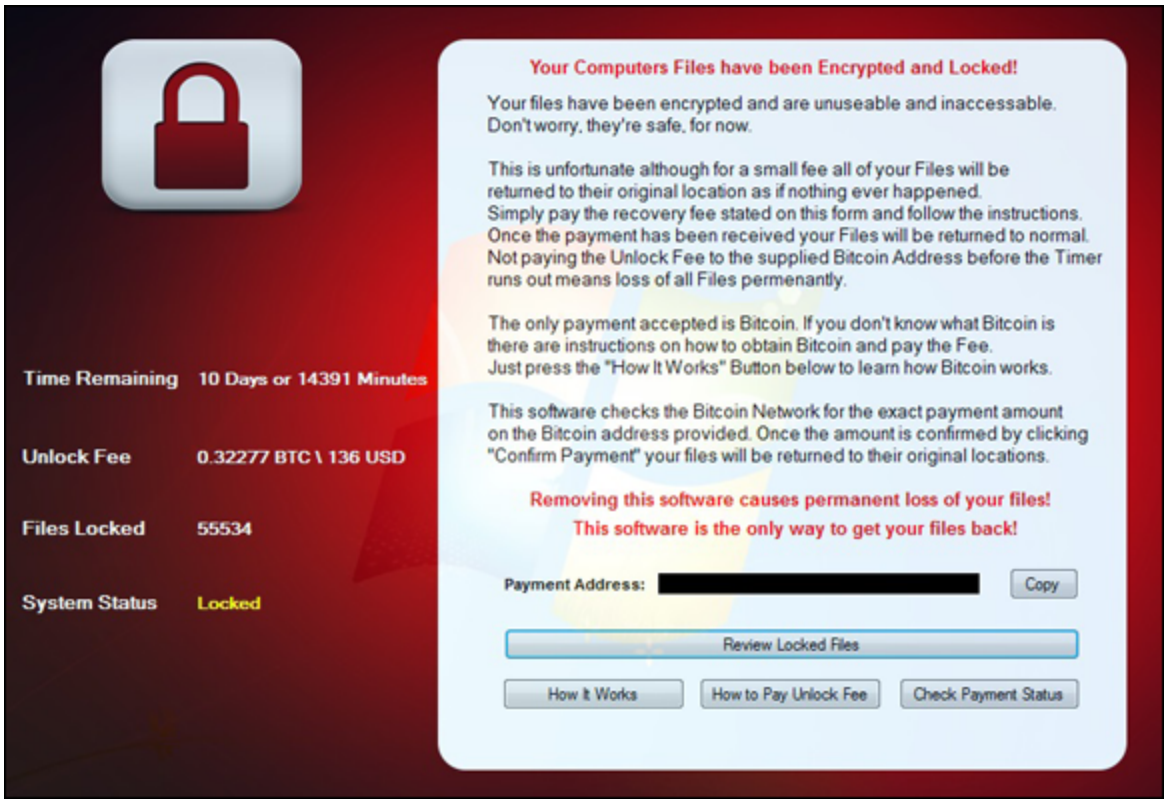

FIGURE 11-1: A ransomware screen from an overt infection.

Obviously, if your device presents you with such a demand and important files that should be accessible to you aren't available because they're missing or encrypted, you can be reasonably sure that you need to take corrective action.

WARNING One note: Some strains of bogus smartphone ransomware — yes, that is a real thing — display such messages but do not actually encrypt, destroy, or pilfer data. Before taking any corrective action, always check that ransomware is real.

Defacement

Defacement refers to breaches in which the attacker defaces the systems of the victim — for example, changing the target's website to display a message that the hacker hacked it (in an almost "virtual subway graffiti"-like sense) or a message of support for some cause, as is often the case with hacktivists (see Figure 11-2).

FIGURE 11-2: A defaced website (ostensibly by the hacker group known as the Syrian Electronic Army).

If you have a personal website and it's defaced or if you boot up your computer and it displays a `hacked by <some hacker>` message, you can be reasonably certain that you were breached and that you need to take corrective action. Of course, the breach may have occurred at the site hosting your site, and not on your local computer — a matter that I discuss in Chapter 12.

Claimed destruction

Hackers can destroy data or programs, but so can technical failures or human errors. The fact that data has been deleted, therefore, doesn't mean that a system was breached. However, if some party claims responsibility, the odds that the problems are the result of a breach can skyrocket.

TIP If someone contacts you, for example, and claims to have deleted a specific file or set of files that only a party with access to the system would know about, and those are the only files gone, you can be reasonably certain that the issue with which you are dealing is not a failure of hard disk sectors or solid-state disk chips.

Detecting Covert Breaches

While some breaches are obviously discernable to be breaches, most breaches are actually quite hard to detect. In fact, breaches are sometimes so hard to notice that various enterprises that spend millions of dollars a year on systems that try to identify breaches have had breaches go undetected for significant periods of time — sometimes for years!

The following sections describe some symptoms that may indicate that your computer, tablet, or smartphone has been breached.

REMEMBER Please keep in mind that none of the following clues exists in a vacuum, nor does the presence of any individual symptom, on its own, provide a guarantee that something is amiss. Multiple reasons other than the occurrence of a breach may cause devices to act abnormally and to exhibit one or more of the ailments described in the following sections.

However, if a device suddenly seems to suffer from multiple suspicious behaviors or if the relevant issues develop just after you clicked on a link in an email or text message, downloaded and ran some software provided by a source with potentially deficient security practices, opened some questionable attachment, or did something else about which wisdom you now question, you may want to take corrective action, as described Chapter 12.

REMEMBER When considering the likelihood that a system was breached, keep in mind relevant circumstances. If problems start occurring after an operating system auto-update, for example, the likely risk level is much lower than if the same symptoms start showing up right after you click on a link in a suspicious email message offering you $1,000,000 if you process a payment being sent from a Nigerian prince to someone in the United States. Maintain a proper perspective and do not panic. If something did go amiss, you can still take action to minimize the damage — see Chapter 12.

Your device seems slower than before

Malware running on a computer, tablet, or smartphone often impacts the performance of the device in a noticeable fashion. Malware that transmits data can also sometimes slow down a device’s connection to the Internet or even to internal networks.

REMEMBER Keep in mind, however, that updates to a device's operating system or to various software packages can also adversely impact the device's performance, so don't panic if you notice that performance seems to be somewhat degraded just after you updated your operating system or installed a software upgrade from a trusted source. Likewise, if you fill up the memory on your device or install many processor and bandwidth intensive apps, performance is likely to suffer even without the presence of malware.

You can see what is running on a Windows PC by pressing Ctrl + Shift + Esc and checking out the Task Manager window that pops up. On a Mac, use the Activity Monitor, which you can access by clicking the magnifying glass on the right side of the menu bar on the top of the screen and starting to type Activity Monitor. After you type the first few characters, the name of the tool should display, at which point you can press Enter to run it.

Your Task Manager doesn't run

If you try to run Task Manager on Windows (see Figure 11-3) or Activity Monitor on a Mac (see preceding section) and the tool does not run, your computer may be infected with malware. Various strains of malware are known to impact the ability of these programs to operate.

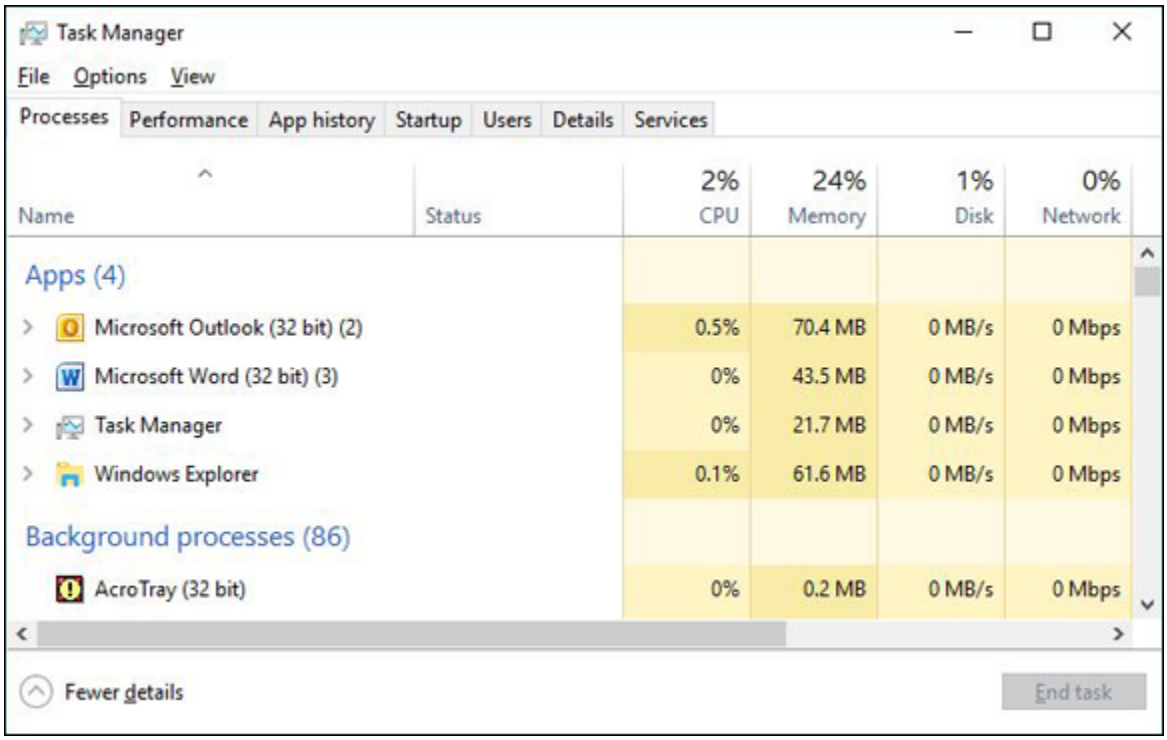

FIGURE 11-3: The Microsoft Windows Task Manager.

Your Registry Editor doesn't run

If you try to run Registry Editor, shown in Figure 11-4, on Windows (for example, by typing **regedit** at the Run prompt) and it does not run, your computer may be infected with malware. Various strains of malware are known to impact the ability of the Registry Editor to execute.

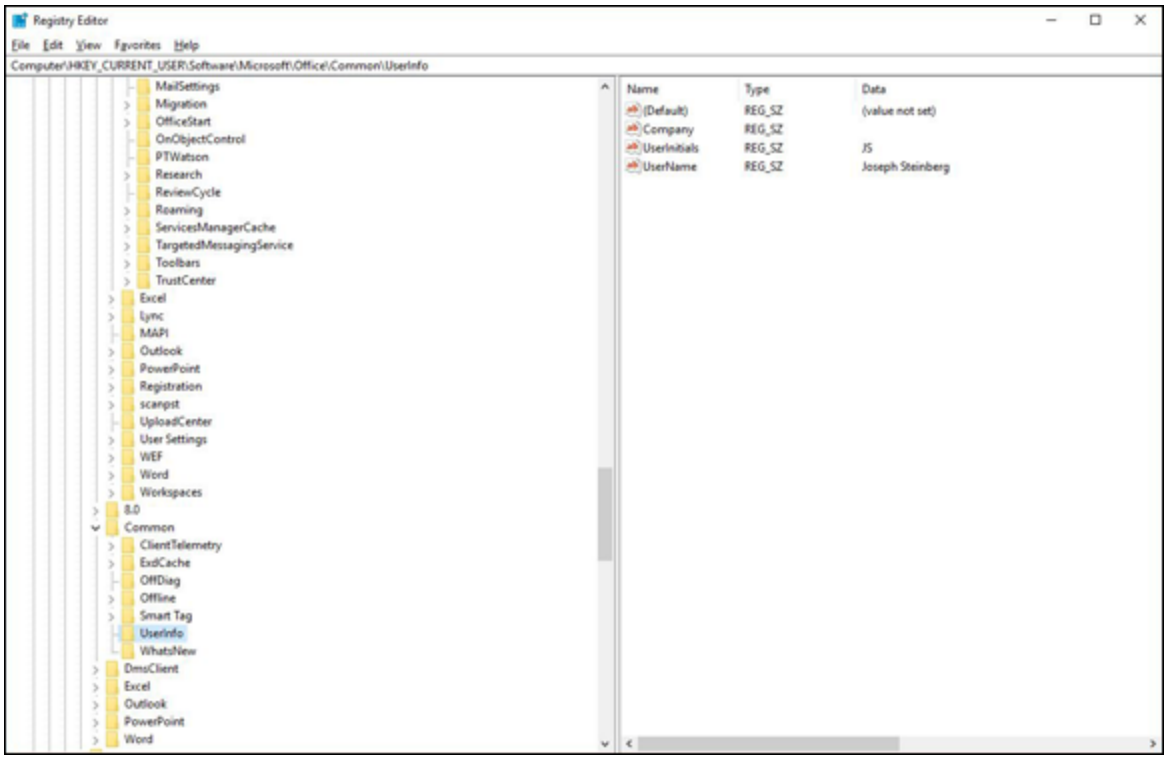

FIGURE 11-4: The Microsoft Windows Registry Editor.

WARNING Note that you may receive a warning when running Registry Editor that it requires Administrator permissions. That warning is normal and not the sign of a problem. It also should remind you of the potentially serious consequences of making registry edits: Don't make any if you're not sure what you are doing.

Your device starts suffering from latency issues

Latency refers to the time it takes for data to begin to travel after the instruction is issued to make it travel. If you're noticing delays that were not present before — especially if the delays seem significant — something may be amiss. Of course, your Internet provider or someone else may be experiencing problems, and everything may be fine on your local device. However, if the latency issues appear from only one device or a particular set of devices and not from all devices connected to the same network and if rebooting the impacted device/s does not ameliorate the situation, your device/s may have been compromised.

TIP If the device is using a wired network connection, be sure to test it with a new cable. If the problem goes away, the cause was likely a defective or damaged physical connection.

Your device starts suffering from communication and buffering issues

One highly visual symptom of communication-performance problems that can easily be discerned without much technical knowledge is if streaming videos seem to freeze while preloading future frames, or *buffering*, far more often than they did in the past (see Figure 11-5). While buffering is an annoyance that happens to most folks from time to time, if it is happening regularly on a connection that previously did not suffer on a regular basis from such an ailment or it's happening from only one or more particular devices using the connection but not on others, it may be indicative of a compromised system.

FIGURE 11-5: An example of communication problems while streaming video. Note the viewable portion of the rotating circle in the middle of the video image.

If the device is using a wired network connection, be sure to check any physical cables that may be causing network issues.

REMEMBER Note that communication performance problems can also be a sign that someone is *piggy-backing* on your Internet connection, which is also a type of breach.

Your device's settings have changed

If you notice that some of your device's settings have changed — and you're certain that you did not make the change — that may be a sign of problems. Of course, some software makes setting changes, too (especially on classic computers, as opposed to smartphones), so changes may have a legitimate source as well. Most software, however, does not make major changes without notifying you. If you see dramatic settings changes, beware.

Your device is sending or receiving strange email messages

If your friends or colleagues report receiving emails from you that you did not send to them, something is likely amiss — this is especially true if the messages appear to be spam. Likewise, if you're receiving emails that appear to be from people who claim to have never sent the relevant messages, you may have suffered a breach.

REMEMBER Keep in mind, however, that many other reasons (including other kinds of attacks on systems other than your own devices and accounts) can lead to spam appearing to have emanated from you.

Your device is sending or receiving strange text messages

If your friends or colleagues report receiving text messages or other smartphone-type communications from you that you did not send to them, your smartphone may have been breached. Likewise, if you're receiving messages that appear to be from people who claim to have never sent the relevant messages, you may have suffered a breach.

New software (including apps) is installed on your device — and you didn't install it

If new programs or apps suddenly appear on your device and you did not install them, something may be amiss. While, in the case of some portable devices, the manufacturer or relevant service provider may occasionally install certain types of apps without your knowledge, if new apps suddenly appear, you should always look into the matter. Do a Google search on the apps and see what reliable tech sites say about them. If the apps are not showing up on other people's devices, you may have a serious issue on your hands.

REMEMBER Keep in mind, however, that sometimes the installation routines of one program install other applications as well. It is relatively common, for example, for various programs that are offered for free to users in a limited-feature version to also install other programs that are comarketed alongside them. Normally, such installation programs ask for permission to install the additional programs, but such transparency is not mandated by law, and some applications do not afford users such choices.

Also, remember that if you let someone else your computer, he or she may have installed something (legitimate or illegitimate).

Your device's battery seems to drain more quickly than before

Malware running in the background uses battery power and can help drain the battery of laptops, smartphones, and tablets.

Your device seems to run hotter than before

Malware running the background uses CPU cycles and can cause a device to run physically hotter than before. You may hear internal cooling fans going on louder or more often than you usually do, or you may feel that the device is physically hotter to the touch.

File contents have been changed

If the contents of files have changed without you changing them and without you running any software that you expect would change them, something may be seriously amiss.

Of course, if you let someone else use your computers and gave him or her access to the files in question, before blaming malware or a hacker, be sure to check with the person you let use the computer whether he or she made any changes.

Files are missing

If files seem to have disappeared without you deleting them and without you running any software that you expect might delete them, something may be seriously amiss.

Of course, technical failures and human mistakes can also cause files to disappear — and, if you let someone else use your computer, he or she may be the culprit.

Websites appear somewhat different than before

If someone has installed malware that is *proxying* on your device — that is, sitting between your browser and the Internet and relaying the communications between them (while reading all the contents of the communications and, perhaps, inserting various instructions of its own) — it may affect how some sites display.

Your Internet settings show a proxy, and you never set one up

If someone has configured your device to use his/her server as a proxy, that party may be attempting to read data sent to and from your device and may try to modify the contents of your session or even seek to hijack it altogether.

Some legitimate programs do configure Internet proxies — but, such proxy information should show up when the software is installed and initially run, not suddenly after you click on a questionable link or download a program from a less-than-trustworthy source. (See Figure 11-6.)

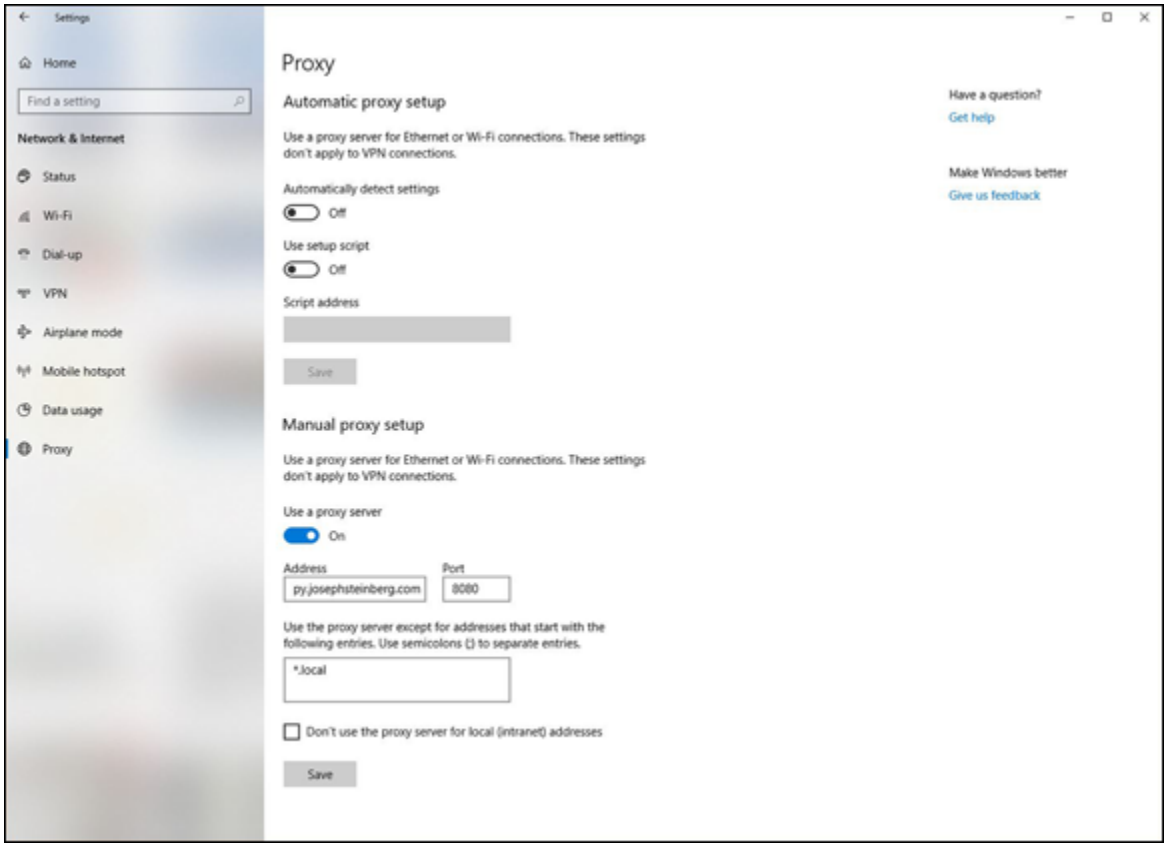

FIGURE 11-6: Internet connections configured to use a proxy. If you do not use a proxy and suddenly one appears listed in your Internet settings, something is likely amiss.

Some programs (or apps) stop working properly

If apps that you know used to work properly on your device suddenly stop functioning as expected, you may be experiencing a symptom of either proxying or malware interfering with the apps' functionality.

TIP Of course, if such a problem develops immediately after you perform an operating system update, the update is a far more likely source of the issue than is something more sinister.

Security programs have turned off

If the security software that you normally run on your device has suddenly been disabled, removed, or configured to ignore certain problems, it may be a sign that a hacker has penetrated your device and has turned off its defenses to prevent both his or her efforts from being blocked as well as to ensure that you do not receive warnings as he or she carries out various additional nefarious activities.

An increased use of data or text messaging (SMS)

If you monitor your smartphone's data or SMS usage and see greater usage figures than you expect, especially if that increase begins right after some suspicious event, it may be a sign that malware is transmitting data from your device to other parties. You can even check your data usage per app — if one of them looks like it is using way too much data for the functionality that it provides, something may be amiss.

WARNING If you installed the app from a third-party app store, you can try deleting the app and reinstalling it from a more trusted source. Keep in mind, however, that if malware is on your device, reinstalling the app may not always fix the problem, even if the app was the original source of the infection.

Increased network traffic

If you monitor your device's Wi-Fi or wired network usage and see greater levels of activity than you expect, especially if that increase begins right after some suspicious event, it may be a sign that malware is transmitting data from your device to other parties.

TIP On some systems, you can even check your data usage per app — if one or more apps look like they are using way too much data for the functionality that they provide, something may be amiss. If you installed the app in question from a less-than-reliable source, you can try deleting the app and reinstalling it from a more trusted source — but if malware is present on your device, reinstalling the app that it brought to the device may not always fix the problem, even if the app was, in fact, the original source of the infection.

You can check how much data your computer is using — and even how much each program is using — by installing a bandwidth monitor program on the device in question.

Unusual open ports

Computers and other Internet-connected devices communicate using virtual ports. Communications for different applications typically enter the device via different ports. Ports are numbered, and most port numbers should always be *closed* — that is, not configured to allow communications in.

TIP If ports that are not normally open on your computer are suddenly open and you did not just install software that could be using such ports, it is usually indicative of a problem. If you use Windows — especially if you understand a little about networking — you can use the built-in `netstat` command to determine which ports are open and what is connecting to your device.

Your device starts crashing

If your computer, tablet, or smartphone suddenly starts to crash on a much more frequent basis than in the past, malware may be running on it. Of course, if you just upgraded your operating system, that is the likely source for the problem.

WARNING If you are regularly seeing screens like the Blue Screen of Death (see Figure 11-7) — or other screens indicating that your computer suffered a fatal error and must be restarted, you have a problem. It may be technical, or it may be due to corruption from malware or a hacker.

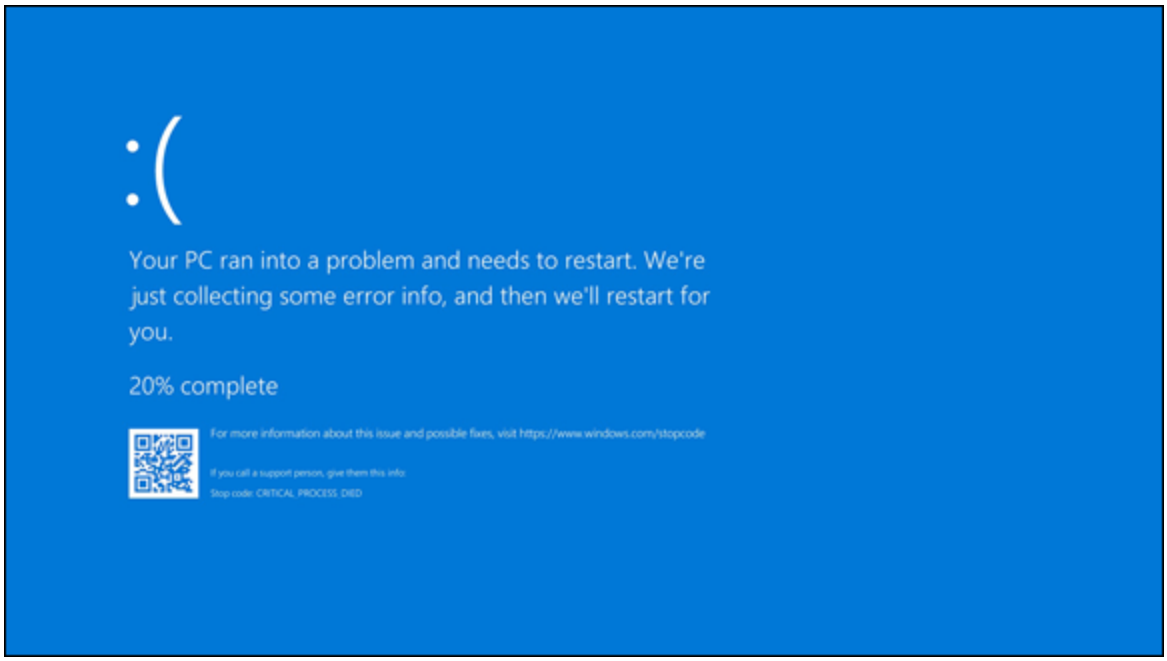

FIGURE 11-7: The modern version of the notorious Blue Screen of Death that appears after a severe crash of a computer running Microsoft Windows 10.

Your cellphone bill shows unexpected charges

Criminals are known to have exploited compromised smartphones in order to make expensive overseas phone calls on behalf of a remote party proxying through the device. Likewise, they can use a breached device to send SMS messages to international numbers and can ring up various other phone charges in other ways.

Unknown programs request access

Most security software for computers warns users when a program first attempts to access the Internet. If you receive such warnings and you don’t recognize the program that is seeking access, or you recognize the

program but can’t understand why it would need to access the Internet (for example, Windows Calculator or Notepad), something may be amiss.

External devices power on unexpectedly

If one or more of your external input devices (including devices such as cameras, scanners, and microphones) seem to power on at unexpected times (for example, when you’re not using them), it may indicate that malware or a hacker is communicating with them or otherwise using them.

There are attacks that are known to have involved criminals remotely turning on people’s cameras and spying on them.

Your device acts as if someone else were using it

Malicious actors sometimes take over computers and use them via remote access almost as if they were sitting in front of the device’s keyboard. If you see your device acting as if someone else is in control — for example, you see the mouse pointer moving or keystrokes being entered while you’re not using your mouse or keyboard — it may be a sign that someone else is actually controlling the machine.

New browser search engine default

As part of several attack techniques, hackers are known to change the default search engine used by people browsing the web. If your own browser’s default search engine changed and you did not change it, something may be amiss. (To check if you’re search engine change, see the list of default applications, as shown in Figure 11-8.)

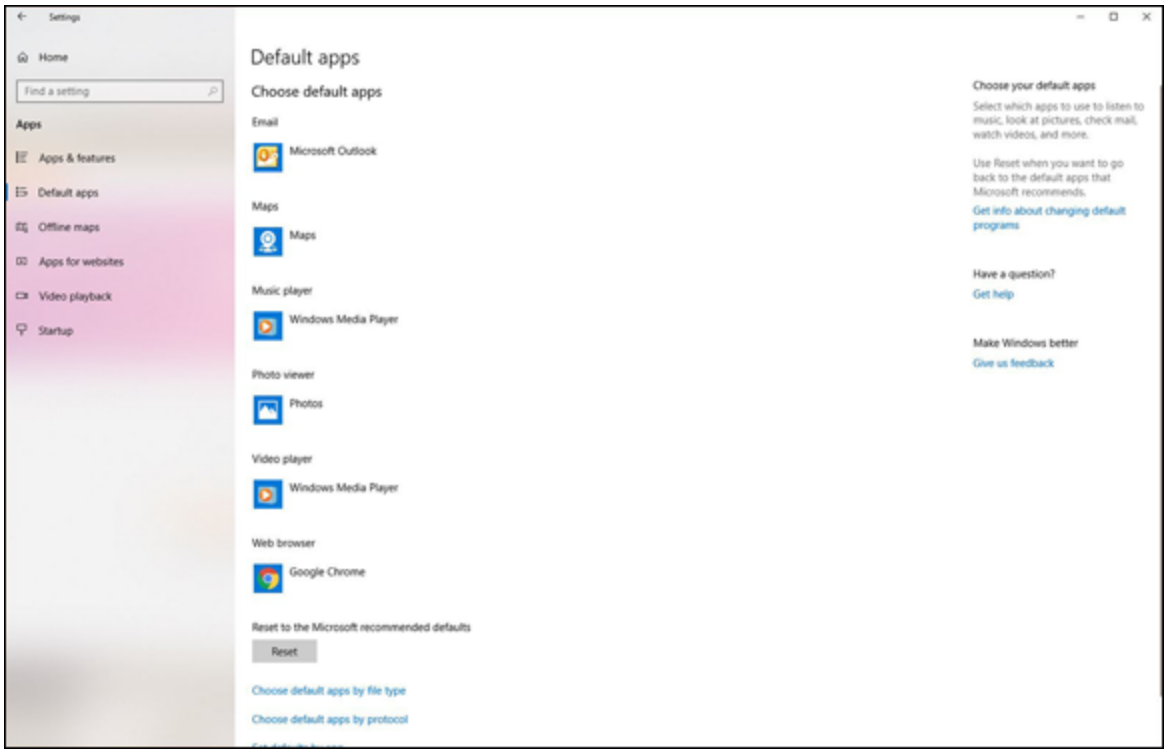

FIGURE 11-8: The Windows 10 Default apps configuration screen.

Your device password has changed

If the password to your phone, tablet, or computer changed without you changing it, something is wrong, and the cause is likely something serious.

Pop-ups start appearing

WARNING Various strains of malware produce pop-up windows asking the user to perform various actions (see Figure 11-9). If you're seeing pop-ups, beware. Such malware is common on laptops, but it exists for some smartphones as well.

FIGURE 11-9: This pop-up window from adware malware attempts to scare people into purchasing bogus security software.

Keep in mind that pop-ups that appear when you're not using a web browser are a big red flag, as are pop-ups advising you to download and install "security software" or to visit websites of questionable repute.

New browser add-ons appear

You should be prompted before any browser add-on is installed (see Figure 11-10). If a new add-on is installed without your knowledge, it likely indicates a problem. Some malware is delivered in poisoned versions of various browser toolbars.

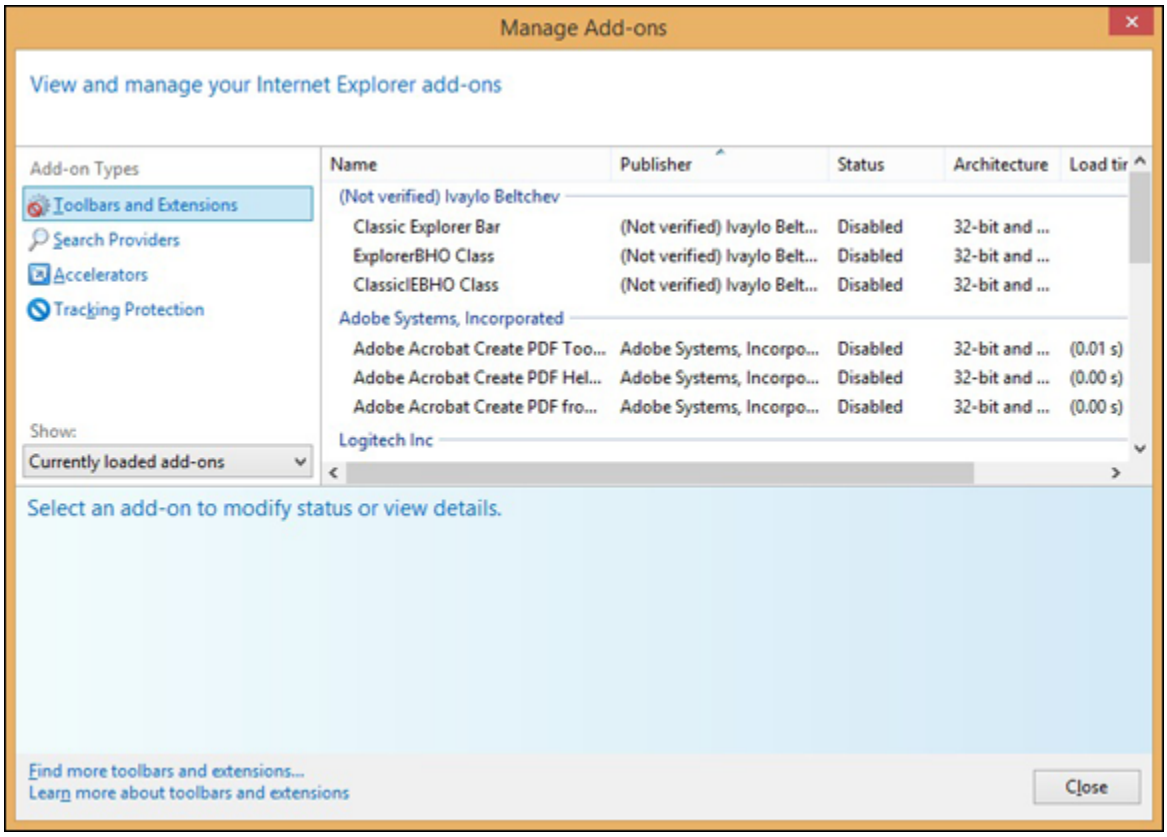

FIGURE 11-10: The Manage Add-ons window in Internet Explorer.

New browser home page

As part of several attack techniques, hackers are known to change the home page of users' browsers. If your own browser's home page changed and you did not change it, something may be amiss.

Your email from the device is getting blocked by spam filters

If email that you send from the device in question used to be able to reach intended recipients with no problem, but is suddenly getting blocked by spam filters, it may be a sign that someone or something altered your email configuration in order to relay your messages through some server that is allowing him or her to read, block, or even modify, your messages, and which other security systems are flagging as problematic.

Your device is attempting to access "bad" sites

If you use your computer, tablet, or smartphone on a network that blocks access to known problematic sites and networks (many businesses, organizations, and government entities have such technology on both their internal and bring-your-own-device [BYOD] networks) and you find out that your device was trying to access such sites without your knowledge, your device is likely compromised.

You're experiencing unusual service disruptions

If your smartphone seems to be suddenly dropping calls, or you find it unable to make calls at times when you appear to have good signal strength, or you hear strange noises during your phone conversations, something may be amiss.

Keep in mind that in most cases, these symptoms are those of technical issues unrelated to a breach. However, in some cases, a breach is the reason for such ailments. So, if you noticed the relevant symptoms shortly after you took some action that you now question or regret, you may want to consider whether you need to take corrective action (see Chapter 12).

Your device's language settings changed

People rarely change the language settings on their computers after performing the initial setup procedure, and few software packages do so either. So, if your computer is suddenly displaying menus and/or prompts in a foreign language or even has a language installed that you never installed, something is likely wrong.

You see unexplained activity on the device

If, on your device, you see emails in your Sent folder that you did not send, your device or email account was likely compromised.

Likewise, if files that you're certain that you never downloaded appear in your Downloads folder, someone else may have downloaded them to your device.

You see unexplained online activity

If your social media account has social media posts that you're certain that neither you nor any app that you have authorized made, something is clearly amiss. It may be that your account was breached, and your devices are all secure, or it may be that one of your devices with access to the account was breached and became the conduit for the unauthorized access to your account.

The same is true if you see videos that you never ordered appearing in your previous rentals of a video streaming service, purchases that you never made appearing in your order history at an online retailer, and so on.

Your device suddenly restarts

While restarts are an integral part of many operating system updates, they should not happen suddenly outside the context of such updates. If your device is regularly rebooting without your approval, something is wrong. The only question is whether the problem emanates from a security breach or from some other issue.

You see signs of data breaches and/or leaks

Of course, if you know that some of your data has leaked, you should try to determine the source of the problem — and the process of checking obviously includes examining for signs of problems on all your smartphones, tablets, and computers.

You are routed to the wrong website

If you're sure that you typed in a correct URL, but were still routed to the wrong website, something is amiss. The problem may reflect a security breach elsewhere, but it could indicate that someone has compromised your device as well.

If the misrouting happens from only one or more particular devices, but not from others on the same network, the odds are that the devices in question were compromised. In any case, never perform any sensitive task (such as logging into a website) from a device that is routing you incorrectly.

Your hard drive light never seems to turn off

If your hard drive light remains on constantly, or near constantly, malware may be doing something to the drive. Of course, hard drive lights come on for legitimate reasons when you are not actively using a computer — and, sometimes, a legitimate reason will entail the light being on for quite some time — so don't panic if it's the only sign that something is amiss.

Other abnormal things happen

It is impossible to list all the possible symptoms that malware can cause a device to exhibit. So, if you keep in mind that parties are seeking to hack into your systems, and that anomalous behavior by your device may be a sign of problems, you increase your odds of noticing when something seems off — and, of properly responding to a breach if one does, in fact, occur.

Chapter 12

Recovering from a Security Breach

IN THIS CHAPTER

- **Surviving when your own computer has been hacked**
- **Recovering when someone has stolen your data from a third-party provider**

You've discovered that you've suffered a data breach. Now what? Read this chapter, which covers how to respond in these types of situations.

An Ounce of Prevention Is Worth Many Tons of Response

REMEMBER When it comes to recovering from a security breach, there simply is no substitute for adequate preparation. No amount of post-breach expert actions will ever deliver the same level of protection as proper pre-breach prevention.

If you follow the various techniques described throughout this book about how to protect your electronic assets, you're likely to be in far better shape to recover from a breach than if you did not. Preparation not only helps you recover, but also helps ensure that you can detect a breach. Without proper preparation, you may not even be able to determine that a breach occurred, never mind contain the attack and stop it. (If you're unsure whether you've suffered a breach, see Chapter 11.)

Stay Calm and Act Now with Wisdom

A normal human reaction to a cyber breach is to feel outraged, violated, and upset and/or to panic, but to properly respond to a breach, you need to think logically and clearly and act in an orderly fashion. Spend a moment to tell yourself that everything will be all right and that the type of attack with which you are dealing is one that most successful people and businesses will likely have to deal with at some point (or at many points).

WARNING Likewise, don't act irrationally. Do not attempt to fix your problem by doing a Google search for advice. Plenty of people online provide bad advice. Even worse, plenty of rogue websites with advice on removing malware and stopping attacks deposit malware on computers accessing them! Obviously, do not download security software or anything else from questionable sites.

Also, keep in mind that you need to act ASAP. Stop whatever else you're doing and focus on fixing the problem. Shut down any programs that you're using, save (and back up onto media that you will scan for malware before you reuse) any open documents and so on, and get to work on recovering from the breach.

REMEMBER When a breach occurs, time works against you. The sooner that you stop someone from stealing your files, corrupting your data, or attacking additional devices on your network, the better off you will be.

Bring in a Pro

Ideally, you should bring in a cybersecurity professional to help you recover. While this book gives you good guidance, when it comes to technical skills, there is simply no substitute for the years of experience that a good pro has.

TIP You should apply the same logic and seek professional help when faced with a serious computer and data crisis as you would if any of the following were true:

- If you were seriously ill, you'd go to the doctor or hospital.
- If you were arrested and charged with a crime, you'd hire a lawyer.
- If the IRS sent you a letter that you're being audited, you'd hire an accountant.

Recovering from a Breach without a Pro's Help

TIP If you do not have the ability to bring in a pro, the following steps are those that you should follow. These steps are essentially the ones most professionals follow:

1. **Figure out what happened (or is happening).**
2. **Contain the attack.**
3. **Terminate and eliminate the attack.**

Step 1: Figure out what happened or is happening

If possible, you want to figure out as much about the attack as possible so that you can respond accordingly. If an attacker is transferring files from your computer to another device, for example, you want to disconnect your device from the Internet ASAP.

That said, most home users do not have the technical skills to properly analyze and understand exactly what the nature of a particular attack may be — unless, of course, the attack is overt in nature (see Chapter 11).

WHEN AN ATTACK GOES UNDETECTED

The lack of expertise in this area by the average person should not be surprising. Most businesses that are breached, including many with their own information security professionals on staff, do not even discover that they have been successfully breached until months after the attackers began attacking! Some experts estimate that, on average, businesses do not discover non-overt information-security compromises until somewhere between six months and a year have elapsed since the initial breach occurred!

Gather as much information as you can about

- What happened
- What information systems and databases were hit
- What could a criminal or other mischievous party do with the stolen material
- What data and programs have been affected
- Who, besides yourself, may face risks because of the breach (this includes any potential implications for your employer)

REMEMBER Do not spend a lot of time on this step — you need to take action, not just document — but the more information that you do have, the greater the chances that you will be able to prevent another similar attack in the future.

Step 2: Contain the attack

Cut off the attacker by isolating him or her from the compromised devices. Containing may entail:

- **Terminating all network connectivity ASAP:** To terminate network connectivity for all devices on a network, turn off your router by unplugging it. (*Note:* If you're in a business setting, this step is usually not possible.)
- **Unplugging any Ethernet cables:** Understand, however, that a network-borne attack may have already spread to other devices on the network. If so, disconnect the network from the Internet and disconnect each device from your network until it is scanned for security problems.
- **Turning off Wi-Fi on the infected device:** Again, a network-borne attack may have already spread to other devices on the network. If so, disconnect the network from the Internet and disconnect each device from your network by turning off Wi-Fi at the router and any access points, not just on the infected computer.
- **Turning off cellular data:** In other words, put your device into airplane mode.
- **Turning off Bluetooth and NFC:** Bluetooth and NFC are both wireless communication technologies that work with devices that are in close physical proximity to one another. All such communications should be blocked if there is a possibility of infections spreading or hackers jumping from device to device.
- **Unplugging USB drives and other removable drives from the system:** *Note:* The drives may contain malware, so do not attach

them to any other systems.

- **Revoking any access rights that the attacker is exploiting:** If you have a shared device and the attacker is using an account other than yours to which he or she somehow gained authorized access, temporarily set that account to have no rights to do anything.

TERMINATING NETWORK CONNECTIVITY

While you can disconnect your Internet connection by physically unplugging from the router or network connection, you can also disable the connection on your device(s).

To terminate network connectivity on a Windows computer, follow these steps:

1. Choose Settings ⇒ Network Connections.
2. Right-click on the relevant connection (or connections one at a time) and then click on Disable.

TIP If, for some reason, you need Internet access from your device in order to get help cleaning it up, turn off all other devices on your network, to prevent any attacks from spreading over the network to your device. Keep in mind that such a scenario is far from ideal. You want to cut off the infected device from the rest of the world, not just sever the connections between it and your other devices.

Step 3: Terminate and eliminate the attack

Containing an attack (see preceding section) is not the same thing as terminating and eliminating an attack. Malware that was present on the infected device is still present after disconnecting the device from the Internet, for example, as are any vulnerabilities that a remote hacker or malware may have exploited in order to take control of your device. So, after containing the attack, it is important to clean up the system.

The following sections describe some steps to follow at this point:

Boot the computer from a security software boot disk

If you have a security software boot disk, boot from it. Most modern users will not have such a disk. If you do not, skip to the next section.

1. **Remove all USB drives, DVDs, CDs, floppies (yes, some people still have them), and any other external drives from your computer.**
2. **Insert the boot disk into the CD/DVD drive.**
3. **Shut down your computer.**
4. **Wait ten seconds and push the power button to start your computer.**
5. **If you are using a Windows computer and it does not boot from the CD, turn the machine off, wait ten seconds, and restart it while pressing the BIOS-boot button (different computers use different buttons, but most use some F-key, such as F1 or F2) to go into the BIOS settings and set it to boot from the CD if a CD is present, before trying to boot from the hard drive.**
6. **Exit the BIOS and Reboot.**

If you're using a Windows PC, boot the computer in Safe Mode. Safe Mode is a special mode of windows that allows only essential system services and programs to run when the system starts up. To do this, follow these steps:

1. **Remove all USB drives, DVDs, CDs, floppies (yes, some people still have them), and any other external drives from your computer.**
2. **Shut down your computer.**
3. **Wait ten seconds and push the power button to start your computer.**
4. **While your computer is starting, press the F8 key repeatedly to display the Boot Options menu.**
5. **When the Boot Options menu appears, select the option to boot in Safe Mode.**

If you're using a Mac, boot it with Safe Boot. MacOS does not provide the full equivalent of Safe Mode. Macs always boot with networking enabled. Its Safe Boot does boot cleaner than a normal boot. To Safe Boot, follow these steps:

1. **Remove all USB drives, DVDs, CDs, floppies (yes, some people still have them), and any other external drives from your computer.**
2. **Shut down your computer.**
3. **Wait ten seconds and push the power button to start your computer.**
4. **While your computer is starting, hold down the Shift key.**

TIP Older Macs (macOS versions 6–9) boot into a special superuser mode without extensions if a user presses the hold key during reboot. The advice to boot with Safe Boot applies only to Macs running more recent operating systems.

Backup

Hopefully you can ignore this section, because you paid attention to the advice in the chapter on backups, but if you have not backed up your data recently, do so now. Of course, backing up a compromised device is not necessarily going to save all your data (because some may already be corrupted or missing), but if you do not already have a backup, do so now — ideally by copying your files to an external USB drive that you will not attach to any other devices until it is properly scanned by security software.

Delete junk (optional)

At this point, you may want to delete any files that you do not need, including any temporary files that have somehow become permanent (a list of such files appears in the chapter on backups).

Why do the deletion now?

Well, you should be doing periodic maintenance, and, if you are cleaning up your computer now, now is a good time. The less there is for security software to scan and analyze, the faster it will run. Also, some malware hides in temporary files, so deleting such files can also directly remove some malware.

For users of Windows computers, one easy way to delete temporary files is to use the built-in Disk Cleanup utility:

1. **In Windows 10, in the search box on the taskbar, type disk cleanup.**
2. **Select Disk Cleanup from the list of results**
3. **Select the drive you want to clean up and then click OK.**
4. **Select the file types to get rid of and then click OK.**
5. **Click on Accessories (or Windows Accessories).**
6. **Click on Disk Cleanup.**

Run security software

Hopefully, you already have security software installed. If you do, run a full system scan. One important caveat: Security software running on a compromised device may itself be compromised or impotent against the relevant threat (after all, the security breach took place with the security software running), so, regardless of whether such a scan comes up clean, it may be wise to run the security software from a bootable CD or other read-only media, or, in cases of some products, from another computer on your home network.

TIP Not all brands of security software catch all variants of malware. Security professionals doing a device “clean up” often run security software from multiple vendors.

If you are using a Mac and your Safe Boot includes Internet access, run the security software update routines prior to running the full scan.

Malware, or attackers, may add new files to a system, remove files, and modify files. They may also open communication ports. Security software should be able to address all of these scenarios. Pay attention to the reports issued by the security software after it runs. Keep track of exactly what it removed or repairs. This information may be important, if, for example, some programs do not work after the cleanup. (You may need to reinstall programs from which files were removed or from which malware-modified files malware was removed.) Email databases may need to be restored if malware was found within messages and the security software was unable to fully clean the mess up.

Security software report information may also be useful to a cybersecurity or IT professional if you end up hiring one at a later date. Also, the information in the report may provide you with clues as to where the attack started and what enabled it to happen, thereby also helping to guide you on preventing it from recurring.

TIP Security Software often detects, and reports about, various non-attack material that may be undesirable due to their impact on privacy or potential to solicit a user with advertisements. You may, for example, see alerts that security software has detected tracking cookies or adware; neither is a serious problem, but you may want to remove adware if the ads bother you. In many cases you can pay to upgrade the software displaying the ads to a paid version that lacks ads. As far as recovering from an attack is concerned, these undesirable items are not a problem.

TIP Sometimes, security software will inform you that you need to run an add-on in order to fully clean a system. Symantec, for example, offers its Norton Power Eraser, that it says “Eliminates deeply embedded and difficult-to-detect crimeware that traditional virus scanning doesn’t always detect.” If your security software informs you that you need to run such a scanner, you should do so, but make sure that you obtain it from the legitimate, official, original source. Also, never download or run any scanner of such a sort if you are told to do so not as the result of running security software. Plenty of rogue pop-ups will advise you similarly, but install malware if you download the relevant “security software.”

Reinstall Damaged Software

There are experts who recommend uninstalling and reinstalling any software package that you know was affected by the attack, even if the security software fixed it.

Restart the system and run an updated security scan

For Windows computers, after you have cleaned the system, restart it in Safe Mode with networking using the procedure described above (but selecting Safe Mode with Networking rather than Safe Mode), run the security software, download all updates, and run the security software scan again.

If there are no updates, then you do not need to rerun the security software.

If you are using a Mac, Safe Boot already included networking so there is no reason to repeat the scan.

Install all relevant updates and patches. If any of your software has not been updated to its latest version and may contain vulnerabilities, fix this

during the cleanup.

TIP If you have the time to do so, run the security software full scan again after you have installed all the updates. There are several reasons for doing so, including the fact that you want it to check your system using its own most-up-to-date information on malware and other threats, as well as the fact that you want its heuristic analysis engine to have a baseline of what the system looks like with its latest updates.

Erase all potentially problematic System Restore points

System Restore is a useful tool, but it can also be dangerous. If a system creates a restore point when malware is running on a device, for example, restoring to that point will likely restore the malware! After cleaning up a system, therefore, be sure to erase all system restore points that may have been created when your system was compromised. If you are unsure if a restore point may be problematic, erase it. For most users, this means that it may be good to erase all system restore points.

To do this:

1. **Click on the Start menu.**
2. **Click on Control Panel.**
3. **Click on All Control Panel Items.**
4. **Click on Recovery.**
5. **Click on Configure System Restore.**
6. **Follow the prompts to delete the relevant system restore points.**

Restoring modified settings

Some attackers and malware may modify various settings on your device. What page you see when you start your web browser — for

example, your web browser home page — is one common item that malware commonly changes. It is important to change the browser page back to a safe page as the malware's starting page might lead to a page that reinstalls malware or performs some other nefarious task.

The following sections walk you through the process for each browser.

REMEMBER When using the phone or tablet versions of the browsers described in the following sections, the process will differ slightly, but should be simply discernable based on the instructions.

IN CHROME

To reset the Chrome browser:

1. **Click on the three-dot menu icon at the top right corner.**
2. **Click on Settings.**
3. **Scroll down to the On Startup section and configure it accordingly.**

IN FIREFOX

To reset the Firefox browser:

1. **Click on the three-line menu icon at the top right corner.**
2. **Click on Options.**
3. **Click on Home.**
4. **Configure the values in the New Windows and Tabs section accordingly**.

IN SAFARI

To reset the Safari browser:

1. **Click on the Safari menu.**
2. **Click on Preferences.**

3. **Click on the General tab.**
4. **Scroll down to the Homepage field and configure it accordingly.**

IN EDGE

To reset the Edge browser:

1. **Click on the three-dot menu icon at the top right corner.**
2. **Click on Settings.**
3. **Configure the Open Microsoft Edge with and Open new tabs with sections accordingly.**

Rebuild the system

Sometimes it is easier, instead of following the aforementioned processes, to simply rebuild the system from scratch. In fact, because of the risk of security software missing some problem, or of user mistakes when performing the security cleanup, many experts recommend that whenever possible one should rebuild a system entirely after a breach.

Even if you plan to rebuild a system in response to a breach, it is still wise to run a security software scan prior to doing so as there are some rare forms of malware that can persist even after a restore (such as BIOS reprogramming malware, certain boot sector viruses, and so on), and to scan all devices on the same network as the compromised device at the time of the compromise or afterwards, so as to ensure that nothing bad can propagate back to the newly restored device.

A guide to rebuilding systems from scratch appears in Chapter 14.

Dealing with Stolen Information

If your computer, phone, or tablet was breached, it is possible that sensitive information on it was stolen and may be misused by a criminal.

You should change any of your passwords that were stored on the device, for example, and check all accounts that were accessible from the device without logging in (due to your earlier setting of the device to

“Remember Me” after a successful login) to ensure that nothing goes wrong. Obviously, if your passwords were stored in a strongly encrypted format the need to change them is less urgent than if they were stored in clear text or with weak encryption, but, ideally, unless you are certain that the encryption will hold up for the long term, you should change them anyway.

If you suspect that information may have been taken that could be used to impersonate you, it may be wise also to initiate a credit freeze and file a police report. Keep a copy of the police report with you. If you are pulled over by a police officer who informs you that there is a warrant out for your arrest in some location where you have never been, for example, you will have proof that you filed a report that private information that could be used to steal your identity was stolen from you. Such a document may not prevent you from having problems entirely, but it certainly may make your situation better in such a scenario than it would be if you had no such proof.

If you believe that your credit or debit card information was stolen, contact the relevant party at the phone number printed on the back of your card, tell them that the number may have been compromised, and ask them to issue you a new card with a new number. Also check the account for any suspicious transactions.

Keep a log of every call you make, when you made it, with whom you spoke, and what occurred on the call.

The more sensitive that information is, the more important it is to take action and to take it quickly.

Here are some ways to think of information:

- **Not private, but can help criminals with identity theft:**
    - Names, address, and home telephone number.

      This type of information is really available to anyone who wants it, even without hacking you. (Consider that a generation ago this type of information was literally published in phone books and sent to every home that had a phone line.)

That said, this type of information can be used in combination with other information to commit all sorts of crimes, especially if unsuspecting other people make mistakes (for example, by allowing someone with this information to open a library card without ever producing identification documents).

- Other public-record information: The price that you paid for your home, the names of your children, and so on. While this information is public record, a criminal correlating it with other information that may be lifted from your computer could create issues for you.

- **Sensitive:** Email addresses, cellphone numbers, credit card account numbers without the CVC code, debit cards account numbers that require a PIN to use or without a CVC code, ATM card numbers, student ID numbers, passport numbers, complete birthdays including the year, and so on. These items create security risks when compromised — for example, a stolen email address may lead to sophisticated phishing attacks that leverage other information garnered from your computer, attempts at hacking into the account, spam emails, and so on. Also, this type of stolen information may be used by a criminal as part of identity theft and financial fraud crimes, but may require combining multiple pieces of information in order to create a serious risk.
- **More sensitive:** Social Security numbers (or their foreign equivalents), passwords to online accounts, bank account numbers (when compromised by a potential criminal as opposed to when displayed on a check given to a trusted party), PINs, credit and debit card information with the CVC code, answers to challenge questions that you have used to secure accounts, and so on. These types of information can often be abused on their own.

Paying ransoms

If you have proper backups, you can remove ransomware the same way that you remove other malware. If any data gets lost in the process, you

can restore it from backups.

If you have been hit with over ransomware and do not have proper backups, however, you may face a difficult decision. Obviously, it is not in the common interest for you to pay a ransom to a criminal in order get your data back, but, in some cases, if your data is important to you, that may be the route that you need to go. In many cases, criminals will not even give you your data back if you do pay the ransom — so, by paying a ransom, you may not only waste money, but still suffer a permanent loss of your data. You will need to decide if you want to take that chance. (Hopefully, this paragraph will serve as a strong motivator for readers to back up proactively as discussed in the chapter on backups.)

Before paying a ransom, consult an information security expert. Some ransomware can be removed, and its effects undone, by various security tools. However, unless your security software tells you that it can undo the encryption done by ransomware, do not try to remove ransomware on your own once it has encrypted your data. Some advanced ransomware wipes the data permanently if it detects attempts to decrypt the data. Also, keep in mind that some advanced ransomware does not encrypt data, but rather removes it from the victim's device and only transmits it back if the ransom is paid. Such ransomware may be removable by security software, but security software cannot usually restore the data pilfered by the ransomware.

TIP The best defense for home users against the impact of ransomware is to back up and keep the backups disconnected from anything else!

Learning for the future

It is important to learn from breaches. If you can figure out what went wrong, and how a hacker managed to get into your systems (either directly or by using malware), you can institute de facto policies and procedures for yourself to prevent future such compromises. A cybersecurity professional may be able to help you vis-à-vis doing so.

Recovering When Your Data Is Compromised at a Third Party

Nearly all Internet users have received notification from a business or government entity (or both) that personal data was potentially compromised. How you address such a scenario depends on many factors, but the following sections tell you the essentials of what you need to know.

Reason the notice was sent

Multiple types of data breaches lead to organizations sending notifications. Not all of them represent the same level of risk to you, however. Notifications may be sent when a company has

- Knowledge that an unencrypted database containing personal information was definitely stolen
- Knowledge that an encrypted database containing personal information was definitely stolen
- Detected unauthorized activity on a computing device housing your information
- Detected unauthorized activity on a computing device, but not the one that houses your information (but on one connected to the same or logically connected network)
- Detected the theft of credit or debit card numbers as can occur with a skimming device or the hacking of a point-of-sale credit card processing device
- Discovered that there were, or may have been, improperly discarded computers, hard drives, or other storage media or paper-based information
- Discovered that there was, or may have been, improperly distributed information, such as sensitive information sent to the wrong parties, unencrypted email sent to authorized parties, and so on

In all these cases, action may be warranted. But if a company notifies you that an unencrypted database of passwords including yours was stolen, the need to act is more urgent than if it detects unauthorized activity on a system on the same network as another machine containing only an encrypted version of your password.

Scams

Criminals see when a breach receives significant attention and often leverage the breach for their own nefarious purposes. One common technique is for crooks to send bogus emails impersonating the breached party. Those emails contain instructions for setting up credit monitoring or filing a claim for monetary compensation for the pain and inconvenience suffered due to the breach. Of course, the links in such messages point to phishing sites, sites that install malware, and other destinations to which you do not want to go.

Criminals also act quickly. In February 2015, for example, the Better Business Bureaus started reporting complaints of emails impersonating Anthem, Inc., less than one day after the health insurance company announced that it had suffered a breach.

Passwords

One of the types of breaches most commonly reported in the mass media involves the theft of password databases.

Modern password authentication systems are designed to provide some protection in case of a breach. Passwords are usually stored in a *hashed format*, meaning that they are stored with one-way encryption. When you enter your password during an attempt to log in, what you type is hashed and then compared with the relevant hash value stored in the password database. As such, your actual password is not stored anywhere and is not present in the password database. If a hacker steals a password database, therefore, the hacker does not immediately obtain your password.

At least that is how things are supposed to work.

In reality, however, not all authentication systems are implemented perfectly; hashed password databases have multiple exploitable weaknesses, some of which can help criminals decipher passwords even when they're hashed. For example, if a criminal looks at the database and sees that the hashed password for many people is the same, it is likely to be a common password (maybe even "password"), which often can be cracked quickly. There are defenses against such attacks, but many authentication systems do not use them.

As such, if you are notified by a company that it has been breached and that an encrypted version of your password was stolen, you should probably reset the password. You don't need to panic, though. In most cases, your password was likely protected by the hashing (unless you selected a common, weak password, which, of course, you should not have). If, for some reason, you have reused the compromised password on other sites that you don't want have unauthorized parties to log in as you, you should reset your password there as well and don't reuse the new password this time!

Payment card information

If your credit card information or debit card information may have been compromised, take the following measures:

- **Leverage credit monitoring services.** Breached firms often give those people potentially affected by the relevant breaches a free year or two of credit monitoring. While one should never rely on such services to provide full protection against identity theft, using such services does have benefit. Being that the cost to you is only a few minutes of time to set up an account, you should probably do so.
- **Monitor your credit reports.** If you see any new accounts that you did not open, immediately contact the party involved. Remember, when it comes to fraud, the earlier that you report a problem, the less aggravation you are likely to suffer from it.
- **Set up text alerts.** If your card issuer offers the capability to set up text alerts, use the feature. That way, you'll be notified when charges are made and can act quickly if something appears to be amiss.

- **Check your monthly statements.** Make sure that you continue to receive your account's statements as you did before and that they are not being misdirected to someone else.
- **Switch to e-statements.** If possible, set up your account to receive electronic monthly statements rather than physical statements and make sure that you receive an email and/or text message when each and every statement is issued. Of course, be sure to properly protect the email account and smartphone to which such messages are sent.

Government-issued documents

If your passport, driver's license, or other government-issued identity document has been compromised, you should contact the agency that issued the relevant document and ask how you should proceed. Document everything that you're told, including details as to who told you what.

You should also check online on the agency's website to see whether it offers instructions for such scenarios. In some cases, agencies will advise you to replace the document, which may necessitate a physical visit to an agency office. In other cases, the agency will advise you to do nothing, but will tag your account so that if the document is used for identification at other government agencies, those checking the ID will know to be extra vigilant (which, in itself, might be a reason to replace the document so that you do not encounter any extra aggravation when using it as ID).

School or employer-issued documents

If your school or employer ID information is compromised, immediately notify the issuer. Not only could this information be used to social engineer your school or employer, but it may potentially be used to obtain sensitive information about you from either one.

Social media accounts

If any of your social media accounts is compromised, immediately contact the relevant social media provider. All major platforms have mechanisms to address stolen accounts because all major platforms have

had to deal with stolen accounts numerous times. Keep in mind that you may be asked to provide government ID to prove your identity as part of the account recovery process.