INTRODUCTION

The field of computing has changed dramatically over the decades since the introduction of the IBM Personal Computer (PC) in 1981, and so has the job of the people who build, maintain, and troubleshoot computers. A *PC tech* for many years serviced IBM-compatible desktop systems running a Microsoft operating system (OS), such as DOS or, later, Windows. All a tech needed to service an early Windows machine was a Phillips-head screwdriver and knowledge of the hardware and OS.

An IBM-compatible PC, circa 1989

The personal computing landscape today includes a zillion devices in all shapes, sizes, and purposes. How many computing devices do you interact

with every day? Seriously, count them.

Here's my typical contact in a day. My smartphone alarm clock awakens me in the morning. I use either a Windows or macOS desktop to check the morning news and my e-mail by connecting to other computers over the Internet. Or, if the family is on both systems, I'll retreat to the study with a laptop running Ubuntu Linux to do the same tasks. At the gym, my smart watch keeps track of my exercises and my heart rate. The computer in my car handles navigation and traffic reports for my daily commute. At the office I'm literally surrounded by dozens of computing devices, because everyone has a desktop or laptop computer, a tablet, a smartphone, plus any number of wearable devices.

We're all PCs!

Someone needs to set up, manage, maintain, and troubleshoot all of these devices. Because you're reading this book, I'm guessing that *you* are that someone. You're going to need a lot of knowledge about many systems to be a modern personal computer technician. A modern *PC tech*, therefore, works with many devices running many different systems. Almost everything interconnects as well, and a PC tech makes that connection happen.

NOTE This book uses the term “personal computer” and the initials “PC” generically to refer to any kind of personal computing device. PCs here mean things that techs interact with, can set up, and repair.

This book teaches you everything you need to know to become a great tech. It might seem like a lot of information at first, but I’ll show you how each system functions and interacts, so you learn the patterns they all follow. At some point in the process of reading this book and working on computers, it will all click into place. You’ve got this!

Along the way, you’ll pick up credentials that prove your skill to employers and clients. The rest of this chapter explains those credentials and the steps you need to take to gain them.

CompTIA A+ Certification

Nearly every profession has some criteria that you must meet to show your competence and ability to perform at a certain level. Although the way this works varies widely from one profession to another, all of them will at some point make you take an exam or series of exams. Passing these exams proves that you have the necessary skills to work at a certain level in your profession, whether you’re an aspiring plumber, teacher, barber, or lawyer.

If you successfully pass these exams, the organization that administers them grants you *certification*. You receive some piece of paper or pin or membership card that you can show to potential clients or employers. This certification gives those potential clients or employers a level of confidence that you can do what you say you can do. Without this certification, either you will not find suitable work in that profession or no one will trust you to do the work.

Modern PC techs attain the *CompTIA A+ certification*, the essential credential that shows competence in the modern field of *information technology (IT)*, a fancy way of saying *computing technology plus all the other stuff needed to connect and support computers*. CompTIA A+ is an industry-wide, vendor-neutral certification program developed and sponsored

by the *Computing Technology Industry Association (CompTIA)*. You achieve this certification by taking two computer-based exams consisting of multiple-choice and performance-based questions. The tests cover what technicians should know after 12 months of hands-on work on personal computing devices, either from a job or as a student in the lab. CompTIA A+ certification enjoys wide recognition throughout the computer industry. To date, more than 1,000,000 technicians have become CompTIA A+ certified, making it the most popular of all IT certifications.

Who Is CompTIA?

CompTIA is a nonprofit industry trade association based in Oakbrook Terrace, Illinois. It consists of over 20,000 members in 102 countries. You'll find CompTIA offices in such diverse locales as Amsterdam, Dubai, Johannesburg, Tokyo, and São Paulo.

CompTIA provides a forum for people in these industries to network (as in meeting people), represents the interests of its members to the government, and provides certifications for many aspects of the computer industry. CompTIA sponsors CompTIA A+, CompTIA Network+, CompTIA Security+, and other certifications. CompTIA works hard to watch the IT industry and constantly looks to provide new certifications to meet the ongoing demand from its membership. Check out the CompTIA Web site at www.comptia.org for details on the other certifications you can obtain from CompTIA.

CompTIA began offering CompTIA A+ certification back in 1993. When it debuted, the IT industry largely ignored CompTIA A+ certification. Since that initial stutter, however, the CompTIA A+ certification has grown to become the de facto requirement for entrance into the PC industry. Many companies require CompTIA A+ certification for all of their PC support technicians, and the CompTIA A+ certification is widely recognized both in the United States and internationally.

The Path to Other Certifications

Most IT companies—big and small—see CompTIA A+ certification as the entry point to IT. Where you go next depends on a lot of things, such as your interests and the needs of your organization. Let's look at other CompTIA

certifications first and then explore vendor-specific options from Microsoft and Cisco.

CompTIA Core Certifications

CompTIA A+ is part of the CompTIA *Core* certifications. Many techs flow from A+ to the others in the Core before specializing. The Core consists of four certifications:

- CompTIA IT Fundamentals (ITF+)
- CompTIA A+ (1001 is called *Core 1*; 1002 is called *Core 2*)
- CompTIA Network+
- CompTIA Security+

CompTIA calls the A+ exams the Core Series (Core 1 and Core 2) to note the two exams.

CompTIA ITF+ covers essentials of computer literacy, such as everything any modern worker needs to know just to function. That includes information about computing device types, what you can do with computers, how networks work, and basic security. If you're already on CompTIA A+, you don't need to backtrack to ITF+. It's good to recommend for newbies, though, as ITF+ will fill in a lot of gaps for people.

CompTIA Network+ continues the good work you started in the CompTIA A+ networking sections. We live in an interconnected world. Techs need to know networking inside and out to handle jobs at bigger organizations. Getting Network+ certified proves your skills as a network tech, including your understanding of network hardware, infrastructure, installation, and troubleshooting. Network+ is the next logical step after A+.

Similarly, *CompTIA Security+* picks up from the network security sections in both A+ and Network+, taking you much deeper into how to secure networks against attacks and best practices for every security-conscious organization. I recommend taking Security+ after Network+; this rounds out your essential skill set all the way up to enterprise tech.

CompTIA Specialty Certifications

CompTIA offers several tracks to pursue post–Core certifications. These offer either specialization in an IT subfield or unique skills measured. Let me explain the Infrastructure Pathway, Cybersecurity Pathway, and Professional Skills tracks.

NOTE For more information about the CompTIA certification pathway and all its certifications, go here: https://certification.comptia.org/certifications/which-certification

Moving to the *Infrastructure Pathway* means turning to the machines and operating systems that beat at the heart of enterprise organizations. There are three certifications in this series:

- CompTIA Linux+
- CompTIA Server+
- CompTIA Cloud+

Many organizations rely on Linux-powered servers to accomplish much of the dedicated hardware tasks. The servers and server infrastructure require specialized knowledge. As much of the industry is moving to cloud-based computing, understanding how to take an organization there successfully is increasingly important for IT professionals.

The *Cybersecurity Pathway* goes deep into the Dark Arts of network security—how to protect *against* bad people, not how to be a successful criminal mastermind—with three certifications:

- CySA+
- Pentest+
- CASP+

These certifications show that you know your skills at analyzing a network of any size, can test for vulnerabilities, and can harden the network dramatically. You can leverage all the information learned in the Core

certifications, using it as the foundation for becoming a security guru.

The *Professional Skills* series offers three exams, but they're geared to unique skillsets used every day in IT:

- Project+
- Cloud Essentials
- CTT+

Project management is wildly important in managing big IT . . . projects. Project managers use this certification to show their credentials. Cloud Essentials is all about what you—not the IT hero, but the business manager—need to know about cloud computing. CTT+ is for people like me, a certification that shows you know how to teach IT skills to adults.

None of the Professional Skills certifications seem obvious or logical to pursue after the Core certifications, but they're situational. If, for example, you find yourself in a position where getting project management credentials will greatly benefit you and your organization, Project+ makes a lot of sense.

Microsoft Technical Certifications

Microsoft operating systems control a huge portion of all installed networks, and those networks need qualified support people to make them run. Pursuing Microsoft's series of certifications for networking professionals is a natural next step after completing the CompTIA certifications. They offer a whole slew of tracks and exams, ranging from specializations in Windows 10 to numerous *Microsoft Certified Solutions Expert (MCSE)* certifications and beyond. You can find more details on the Microsoft Learning Web site:

www.microsoft.com/learning

Cisco Certification

Cisco routers pretty much run the Internet and most intranets in the world. A *router* is a networking device that controls and directs the flow of information over networks, such as e-mail messages, Web browsing, and so on. Cisco provides multiple levels of IT certification for folks who want to show their skills at handling Cisco products, such as the *Cisco Certified*

Network Associate (CCNA), plus numerous specialty certifications. See the Cisco IT Certification Web site here for more details:

www.cisco.com/web/learning/certifications

CompTIA A+ Objectives

CompTIA splits A+ certification into two exams: *CompTIA A+ 220-1001* and *CompTIA A+ 220-1002*. It's common to refer to these two exams as the "2019" exams, but CompTIA is also now referring to them as Core 1 and Core 2.

Although you may take either of the two exams first, I recommend taking 220-1001 followed by 220-1002. The 220-1001 exam concentrates on understanding terminology and technology, how to do fundamental tasks such as upgrading RAM, and basic network and mobile device support. The 220-1002 exam builds on the first exam, concentrating on operating system support, advanced configuration, and troubleshooting scenarios.

Both of the exams are extremely practical, with little or no interest in theory, aside from troubleshooting. All questions are multiple-choice, simulation, or "click on the right part of the picture" questions. The following is an example of the type of questions you will see on the exams:

Your laser printer is printing blank pages. Which item should you check first?

A. Printer drivers
B. Toner cartridge
C. Printer settings
D. Paper feed

The correct answer is B, the toner cartridge. You can make an argument for any of the others, but common sense (and skill as a PC technician) tells you to check the simplest possibility first.

The 2019 exams use a regular test format in which you answer a set number of questions and are scored based on how many correct answers you give. CompTIA makes changes and tweaks over time, so always check the CompTIA Web site before final preparation for the exams. These exams have

no more than 90–100 questions each.

Be aware that CompTIA may add new questions to the exams at any time to keep the content fresh. The subject matter covered by the exams won't change, but new questions may be added periodically at random intervals. This policy puts strong emphasis on understanding concepts and having solid PC-tech knowledge rather than on trying to memorize specific questions and answers that may have been on the tests in the past. No book or Web resource will have all the "right answers" because those answers change constantly. Luckily for you, however, this book not only teaches you what steps to follow in a particular case, but also explains how to be a knowledgeable tech who understands *why* you're doing those steps. That way, when you encounter a new problem (or test question), you can work out the answer. This will help you pass the exams and function as a master tech.

Windows-Centric

The CompTIA A+ exams cover six different operating systems and many versions within each OS. When you review the objectives a little later in this section, though, you'll see that the majority of content focuses on the Microsoft Windows operating systems you would expect to find on a PC at a workstation or in a home. The exams cover a specific and limited scope of questions on macOS, Linux, Chrome OS, iOS, and Android. You might even get a question on Windows Phone.

Objectives in the exams cover the following operating systems:

- Windows 7 Starter, Windows 7 Home Premium, Windows 7 Professional, Windows 7 Ultimate, Windows 7 Enterprise
- Windows 8, Windows 8 Pro, Windows 8 Enterprise
- Windows 8.1, Windows 8.1 Pro, Windows 8.1 Enterprise
- Windows 10 Home, Windows 10 Pro, Windows 10 Enterprise
- macOS
- Linux
- Chrome OS
- iOS
- Android

Try This! Recommending an OS

Imagine this scenario. One of your first clients wants to upgrade her computing gear and doesn't know which way to go. It's up to you to make a recommendation. This is a great way to assess your knowledge at the start of your journey into CompTIA A+ certification, so try this!

Open a Web browser on a computer or smartphone and browse to my favorite tech store, Newegg (www.newegg.com). Scan through their computer systems. What operating systems seem to be most common? What can you get from reading reviews of, say, Chrome OS vs. Windows 10? Do they sell any Apple products?

Don't get too wrapped up in this exercise. It's just a way to ease you into the standard research we techs do all the time to stay current. We'll revisit this exercise in later chapters so you can gauge your comfort and knowledge level over time.

Exam 220–1001

The questions on the CompTIA A+ 220-1001 exam fit into one of five domains. The number of questions for each domain is based on the percentages shown in the following table.

Domain (Exam 220-1001)	Percentage
1.0 Mobile Devices	14%
2.0 Networking	20%
3.0 Hardware	27%
4.0 Virtualization and Cloud Computing	12%
5.0 Hardware and Network Troubleshooting	27%

The 220-1001 exam tests your knowledge of computer components, expecting you to be able to identify just about every common device on PCs, including variations within device types. Here's a list:

- Hard drives
- Optical drives
- Solid-state drives (SSDs)

- Motherboards
- Power supplies
- CPUs
- RAM
- Monitors
- Input devices, such as keyboards, mice, and touchscreens
- Video and multimedia cards
- Network and modem cards
- Cables and connectors
- Heat sinks, fans, and liquid cooling systems
- Laptops and mobile devices
- Printers and multifunction devices
- Scanners
- Network switches, cabling, and wireless adapters
- Biometric devices
- Virtualization
- Cloud computing

The 220-1001 exam tests your ability to install, configure, and maintain all the hardware technology involved in a personal computer. You need to be able to install and set up a hard drive, for example, and configure devices in Windows 7, Windows 8, Windows 8.1, and Windows 10. You have to understand device drivers.

The 220-1001 exam tests you on mobile devices. While the smartphone and tablet market covers an impossibly wide array of hardware and software, the 220-1001 exam focuses on Apple iOS and Google Android devices (though you might get a question on Google Chrome OS or Windows Phone). You'll need to know how to interact with the hardware and software.

The 220-1001 exam tests extensively on networking. You need to know how to set up a typical local area network (LAN), for example, understanding cabling standards, network protocols, and Windows configuration.

The 220-1001 exam will quiz you on cloud computing and virtualization technologies. You'll need to know about available cloud services such as online storage and applications only available via the Internet. You'll get

asked how to set up and maintain virtual machines in a network environment.

The 220-1001 exam requires you to know a lot about hardware and network troubleshooting. You'll get questions, for example, on how to fix a network failure.

Exam 220-1002

The CompTIA A+ 220-1002 exam covers four domains. This table lists the domains and the percentage of questions dedicated to each domain.

Domain (Exam 220-1002)	Percentage
1.0 Operating Systems	27%
2.0 Security	24%
3.0 Software Troubleshooting	26%
4.0 Operational Procedures	23%

The 220-1002 exam covers the configuration, repair, and troubleshooting of operating systems—primarily Microsoft Windows, but you'll also get questions on Apple macOS, various Linux distributions, and Google Chrome OS. You have to know your way around Windows and understand the tasks involved in updating, upgrading, and installing Windows 7, Windows 8, Windows 8.1, and Windows 10. You need to know the standard diagnostic tools available in Windows so that you can fix problems and work with higher-level techs. Make sure you know Windows; probably a quarter of the questions are going to challenge you on this.

You need to know your way around the Linux and macOS interfaces. Plus, the 220-1002 exam tests you on accessing and properly using various tech tools for running maintenance, backup, and so forth. The exam goes into lots of detail on iOS and Android configuration, such as setting up e-mail and securing the devices. But it's not just mobile devices . . .

In general, security is a big topic on the 220-1002 exam. You need to know quite a bit about computer security, from physical security (door locks to retinal scanners), to knowledge of security threats (malware and viruses), to the ways in which to secure an individual computer. This also includes coverage of how to recycle and dispose of computer gear properly.

You'll also be tested on methods for securing networks. You'll need to know how to access a small office/home office (SOHO) router or wireless

access point and configure that device to protect your network.

Additionally, this exam puts a lot of emphasis on operational procedures, such as safety and environmental issues, communication, and professionalism. You need to understand how to avoid hazardous situations. The exam tests your ability to communicate effectively with customers and coworkers. You need to understand professional behavior and demonstrate that you have tact, discretion, and respect for others and their property.

The Path to Certification

You become CompTIA A+ certified, in the simplest sense, by taking and passing two computer-based exams. There are no prerequisites for taking the CompTIA A+ certification exams (although there's an assumption of computer literacy, whether or not you have one of the computer literacy certifications). There is no required training course and no training materials to buy. You *do* have to pay a testing fee for each of the two exams. You pay your testing fees, go to a local testing center, and take the tests. You immediately know whether you have passed or failed. By passing both exams, you become CompTIA A+ certified.

To stay certified, every three years you'll need to either retake the exam or perform sufficient continuing education as specified by CompTIA.

Retaking the exams isn't that hard to understand, but the continuing education requirement is a bit more complex. Instead of trying to explain it all here, please review CompTIA's documentation:

https://certification.comptia.org/continuing-education

Most importantly, if you pursue the continuing education path, you'll need to earn 20 continuing education units (CEUs) each three-year period to renew your CompTIA A+ certification. How do you earn these CEUs? You can participate in industry events and seminars, complete a presentation, participate in IT training, teach a course, or earn another higher-level certification. The number of CEUs that you earn by completing each of these requirements varies, and each requires that you submit documentation to CompTIA for review.

Finding a Testing Center

Pearson VUE administers the CompTIA A+ testing at over 5000 testing centers in 165 countries. You may take the exams at any testing center. You can select the closest training center and schedule your exams right from the comfort of your favorite Web browser by going to the Pearson VUE Web site:

www.vue.com

Alternatively, in the United States and Canada, call Pearson VUE at 877-551-PLUS (7587) to schedule the exams and to locate the nearest testing center. International customers can find a list of Pearson VUE international contact numbers for various regions of the world on their Web site here:

www.pearsonvue.com/comptia/contact/

You must pay for the exam when you call to schedule. Be prepared to sit on hold for a while. Have your Social Security number (or international equivalent) and a credit card ready when you call. Pearson VUE will be glad to invoice you, but you won't be able to take the exam until they receive full payment.

Pearson VUE will accommodate any special needs, although this may limit your selection of testing locations.

Exam Costs

The cost of the exam depends on whether you work for a CompTIA member or not. At this writing, the cost for non-CompTIA members is $219 (U.S.) for each exam. International prices vary, but you can check the CompTIA Web site for international pricing. Of course, the prices are subject to change without notice, so always check the CompTIA Web site for current pricing.

Very few people pay full price for the exam. Virtually every organization that provides CompTIA A+ training and testing also offers discount *vouchers*. You buy a discount voucher and then use the voucher number instead of a credit card when you schedule the exam. Vouchers are sold per exam, so you'll need two vouchers to take the two CompTIA A+ exams.

Total Seminars is one place to get discount vouchers. You can call Total Seminars at 800-446-6004 or 281-922-4166, or get vouchers via the Web site: www.totalsem.com. No one should ever pay full price for CompTIA A+ exams.

How to Pass the CompTIA A+ Exams

CompTIA designed the A+ exams to test the knowledge of a technician with only 12 months of experience, so keep it simple! The exams aren't interested in your ability to overclock DDR4 CAS latency in system setup or whether you can explain the differences between Intel and AMD chipsets. Think in terms of practical knowledge and standards. Read this book, do whatever works for you to memorize the key concepts and procedures, take the practice exams on the media accompanying this book, review any topics you miss, and you should pass with no problem.

NOTE Those of you who just want more knowledge in managing and troubleshooting PCs can follow the same strategy as certification-seekers. Think in practical terms and work with the PC as you go through each chapter.

Some of you may be in or just out of school, so studying for exams is nothing novel. But if you haven't had to study for and take an exam in a while, or if you think maybe you could use some tips, you may find the next section valuable. It lays out a proven strategy for preparing to take and pass the CompTIA A+ exams. Try it. It works.

Obligate Yourself The very first step you should take is to schedule yourself for the exams. Have you ever heard the old adage, "Heat and pressure make diamonds?" Well, if you don't give yourself a little "heat," you'll end up procrastinating and delay taking the exams, possibly forever. Do yourself a favor. Using the following information, determine how much time you'll need to study for the exams, and then call Pearson VUE or visit

their Web site and schedule the exams accordingly. Knowing the exams are coming up makes it much easier to put down the game controller and crack open the book. You can schedule an exam as little as a few weeks in advance, but if you schedule an exam and can't take it at the scheduled time, you must reschedule at least a day in advance or you'll lose your money.

Set Aside the Right Amount of Study Time After helping thousands of techs get their CompTIA A+ certification, we at Total Seminars have developed a pretty good feel for the amount of study time needed to pass the CompTIA A+ certification exams. The following table provides an estimate to help you plan how much study time you must commit to the CompTIA A+ certification exams. Keep in mind that these are averages. If you're not a great student or if you're a little on the nervous side, add 10%; if you're a fast learner or have a good bit of computer experience, you may want to reduce the figures.

To use the table, just circle the values that are most accurate for you and add them up to get your estimated total hours of study time.

	Amount of Experience			
Tech Task	**None**	**Once or Twice**	**Every Now and Then**	**Quite a Bit**
Installing an adapter card	6	4	2	1
Installing and configuring hard drives and SSDs	10	8	6	2
Connecting a computer to the Internet	8	6	4	2
Installing printers and multifunction devices	16	8	4	2
Installing RAM	8	6	4	2
Installing CPUs	8	7	5	3
Repairing printers	6	5	4	3
Repairing boot problems	8	7	7	5
Repairing portable computers	8	6	4	2
Configuring mobile devices	4	3	2	1
Building complete systems	12	10	8	6
Using the command line	8	8	6	4
Installing and optimizing Windows	10	8	6	4
Using Windows 7	6	6	4	2

Using Windows 8/8.1	8	6	4	2
Using Windows 10	8	6	4	2
Using Linux	8	6	6	3
Using macOS	8	4	4	2
Configuring NTFS, Users, and Groups	6	4	3	2
Configuring a wireless network	6	5	3	2
Configuring a software firewall	6	4	2	1
Using cloud services	3	2	2	1
Removing malware	4	3	2	0
Using OS diagnostic tools	8	8	6	4
Installing and configuring virtual machines	6	4	2	1

To that value, add hours based on the number of months of direct, professional experience you have had supporting PCs, as shown in the following table.

Months of Direct, Professional Experience	Hours to Add to Your Study Time
0	50
Up to 6	30
6 to 12	10
Over 12	0

A total neophyte often needs roughly 240 hours of study time. An experienced tech shouldn't need more than 60 hours.

Total hours for you to study: _____.

A Strategy for Study Now that you have a feel for how long it's going to take to prepare for the exams, you're ready to develop a study strategy. I suggest a strategy that has worked for others who've come before you, whether they were experienced techs or total newbies.

This book accommodates the different study agendas of these two groups of students. The first group is experienced techs who already have strong PC experience but need to be sure they're ready to be tested on the specific subjects covered by the CompTIA A+ exams. The second group is those with little or no background in the computer field. These techs can benefit from a more detailed understanding of the history and concepts that underlie modern PC technology, to help them remember the specific subject matter

information they must know for the exams. I'll use the shorthand terms Old Techs and New Techs for these two groups. If you're not sure which group you fall into, pick a few chapters and go through some end-of-chapter questions. If you score less than 70%, go the New Tech route.

I have broken most of the chapters into four distinct parts:

- **Historical/Conceptual** Topics that are not on the CompTIA A+ exams but will help you understand more clearly what is on the CompTIA A+ exams
- **1001** Topics that clearly fit under the CompTIA A+ 220-1001 exam domains
- **1002** Topics that clearly fit under the CompTIA A+ 220-1002 exam domains
- **Beyond A+** More advanced issues that probably will not be on the CompTIA A+ exams—yet

The beginning of each of these parts is clearly marked with a large banner that looks like this:

Historical/Conceptual

Those of you who fall into the Old Tech group may want to skip everything except the 1001 and 1002 parts in each chapter. After reading the sections in those parts, jump immediately to the questions at the end of the chapter. The end-of-chapter questions concentrate on information in the 1001 and 1002 sections. If you run into problems, review the Historical/Conceptual sections in that chapter. Note that you may need to skip back to previous chapters to get the Historical/Conceptual information you need for later chapters.

After going through every chapter as described, Old Techs can move directly to testing their knowledge by using the free practice exams on the media that accompanies the book. Once you start scoring above 90%, you're ready to take the exams. If you're a New Tech—or if you're an Old Tech who wants the full learning experience this book can offer—start by reading the book, *the whole book*, as though you were reading a novel, from page one to the end without skipping around. Because so many computer terms and concepts build on each other, skipping around greatly increases the odds that

you will become confused and end up closing the book and firing up your favorite game. Not that I have anything against games, but unfortunately that skill is *not* useful for the CompTIA A+ exams!

Your goal on this first read is to understand concepts, the *whys* behind the *hows*. Having a PC nearby as you read is helpful so you can stop and inspect the PC to see a piece of hardware or how a particular concept manifests in the real world. As you read about hard drives, for example, inspect the cables. Do they look like the ones in the book? Is there a variation? Why? It is imperative that you understand why you are doing something, not just how to do it on one particular system under one specific set of conditions. Neither the exams nor real life as a PC tech will work that way.

If you're reading this book as part of a managing and troubleshooting PCs class rather than a certification-prep course, I highly recommend going the New Tech route, even if you have a decent amount of experience. The book contains a lot of details that can trip you up if you focus only on the test-specific sections of the chapters. Plus, your program might stress historical and conceptual knowledge as well as practical, hands-on skills.

The CompTIA A+ certification exams assume that you have basic user skills. The exams really try to trick you with questions on processes that you may do every day and not think much about. Here's a classic: "To move a file from the C:\DATA folder to the D:\ drive using File Explorer, what key must you hold down while dragging the file?" If you can answer that without going to your keyboard and trying a few likely keys, you're better than most techs! In the real world, you can try a few wrong answers before you hit on the right one, but for the exams, you have to *know* it. Whether Old Tech or New Tech, make sure you are proficient at user-level Windows skills, including the following:

- Recognizing all the components of the standard Windows desktop (Start menu, notification area, etc.)
- Manipulating windows—resizing, moving, and so on
- Creating, deleting, renaming, moving, and copying files and folders within Windows
- Understanding file extensions and their relationship with program associations
- Using common keyboard shortcuts/hotkeys

- Installing, running, and closing a Windows application

When you do your initial read-through, you may be tempted to skip the Historical/Conceptual sections—don't! Understanding the history and technological developments behind today's personal computing devices helps you understand why they work—or don't work—the way they do. Basically, I'm passing on to you the kind of knowledge you might get by apprenticing yourself to an older, experienced PC tech.

After you've completed the first read-through, go through the book again, this time in textbook mode. If you're an Old Tech, start your studying here. Try to cover one chapter at a sitting. Concentrate on the 1001 and 1002 sections. Get a highlighter and mark the phrases and sentences that bring out major points. Be sure you understand how the pictures and illustrations relate to the concepts being discussed.

Once you feel you have a good grasp of the material in the book, you can check your knowledge by using the practice exams included on the media accompanying this book. You can take these in Practice mode or Final mode. In Practice mode, you can use the Assistance window to get a helpful hint for the current questions, use the Reference feature to find the chapter that covers the question, check your answer for the question, and see an explanation of the correct answer. In Final mode, you answer all the questions and receive an exam score at the end, just like the real thing. You can also adjust the number of questions on a Practice or Final mode exam with the Customize option.

Both modes show you an overall grade, expressed as a percentage, as well as a breakdown of how well you did on each exam domain. The Review Questions feature lets you see which questions you missed and what the correct answers are. Use these results to guide further studying. Continue reviewing the topics you miss and taking additional exams until you are consistently scoring in the 90% range. When you get there, you are ready to pass the CompTIA A+ certification exams.

Study Tactics

Perhaps it's been a while since you had to study for a test. Or perhaps it hasn't, but you've done your best since then to block the whole experience from your mind. Either way, savvy test-takers know that certain techniques

make studying for tests more efficient and effective.

Here's a trick used by students in law and medical schools who have to memorize reams of information: Write it down. The act of writing something down (not typing, *writing*) in and of itself helps you to remember it, even if you never look at what you wrote again. Try taking separate notes on the material and re-creating diagrams by hand to help solidify the information in your mind.

Another oldie but goodie: Make yourself flash cards with questions and answers on topics you find difficult. A third trick: Take your notes to bed and read them just before you go to sleep. Many people find they really do learn while they sleep!

Contact

If you have any problems, any questions, or if you just want to argue about something, feel free to send an e-mail to the author (michaelm@totalsem.com) or to the editor (scottj@totalsem.com).

For any other information you might need, contact CompTIA directly at their Web site: www.comptia.org.

CHAPTER 1

Safety and Professionalism

In this chapter, you will learn how to

- Present yourself with a proper appearance and professional manner
- Talk to customers in a professional, productive manner
- Discuss the tools of the trade and preparations necessary to deal with problems proactively

I am a “nerd” and I consider the term a compliment. Nerds are smart and like to work with technology—these are the good aspects of nerd-dom. On the other hand, many people think of the term nerd as an insult. Nerds are rarely portrayed in a positive manner in the media, and I think I know why. Nerds generally suffer from some pretty serious social weaknesses. These weaknesses are classics: bad clothing, shyness, and poor communication skills. If you’ve ever seen an episode of the TV show *The Big Bang Theory*, you know what I’m talking about.

This chapter covers some basic life skills to enable you to enjoy your nerdiness and yet function out in the real world. You’ll learn how to act as a professional and how to communicate effectively. After you’re well on your way to the beginnings of social graces, we’ll discuss some of the hazards (such as static electricity) you may run into in your job and the tools you can use to prevent problems. After all, nerds who cannot stay organized—or who break equipment or themselves—need to learn some tricks to keep everything organized and safe. The chapter finishes with a discussion about troubleshooting. You’ll learn the CompTIA A+ troubleshooting methodology, an excellent tool that will serve you well in your studies and career as a tech.

1002

The Professional Tech

A professional tech displays professionalism, which might seem a little trite if it weren't absolutely true. The tech presents a professional appearance and follows a proper ethical code. I call the latter the Traits of a Tech. Let's look at these two areas in more detail.

Appearance

Americans live in a casual society. The problem with casual is that perhaps our society is becoming *too* casual. Customers often equate casual clothing with a casual attitude. You might think you're just fixing somebody's computer, but you're doing much more than that. You are saving precious family photos. You are keeping a small business in operation. This is serious stuff, and nobody wants an unclean, slovenly person doing these important jobs. Look at Figure 1-1. This is our resident illustrator (among other job descriptions), Ford Pierson, casually dressed to hang with his buddies.

Figure 1-1 Casual Ford

I have a question for you. If you ran a small business and your primary file server died, leaving 15 employees with nothing to do, how would you feel about Ford as a tech coming into your office looking like this? I hope your answer would be “not too confident.” Every company has some form of dress code for techs. Figure 1-2 shows Ford dressed in a fairly typical example, with a company polo shirt, khaki pants, and dark shoes (trust me on that score). Please also note that both his shirt and his pants are wrinkle free. All techs either know how to iron or know the location of the nearest cleaners.

While we are looking at this model of a man, do you appreciate that his hair is combed and his face is cleanly shaven? It’s too bad I can’t use scratch-and-sniffs, but if I could, you’d also notice that Professional Ford took a shower, used some deodorant, and brushed his teeth.

I hope that most of the people who read this smile quietly to themselves

and say, “Well, of course.” The sad truth tells me otherwise. Next time you look at a tech, ask yourself how many of these simple appearance and hygiene issues were missed. Then make a point not to be one of the unkempt techs.

Figure 1-2 Professional Ford

The Traits of a Tech

When I was a Boy Scout in the United States, we learned something called the Boy Scout Law, a list of traits that define the ethics of a Boy Scout. Even though I haven’t been active in Boy Scouts for a long time, I still have the Scout Law memorized: “A Scout is trustworthy, loyal, helpful, friendly, courteous, kind, obedient, cheerful, thrifty, brave, clean, and reverent.”

My goal here isn’t a sales pitch for scouting in any form, but rather to give

you an idea of what we are trying to achieve: a list of ethics that will help you be a better technician. The list you are about to see is my own creation, but it does a great job of covering the CompTIA A+ objectives. Let's dive into the traits of a tech: honesty/integrity, dependability/responsibility, and sensitivity.

Honesty/Integrity

Honesty and integrity are not the same thing, but for a tech, they are so closely related that it is best to think of them as one big ethic. *Honesty* means to tell the truth, and *integrity* means doing the right thing.

It's simple to say you have to be honest, but be warned that our industry often makes it difficult. IT technicians get a lot of leeway compared to most starting jobs, making dishonesty tempting. One of the biggest temptations is lying to your boss. A new tech driving around in a van all day may find it convenient to stretch the truth on how long he took for lunch or how far along he is on the next job. Being up front and honest with your boss is pretty obvious and easy to understand.

Being honest with your customers is a lot harder. Don't sell people goods and services they don't need, even if you get a cut of what you sell. Don't lie to your customers about a problem. If you can't explain the problem to them in plain English, don't create techno-babble (see note) and don't be afraid to say, "I don't know." Too many techs seem to think that not knowing exactly what a problem might be reflects poor skill. A skilled tech can say "I don't know, but I know how to figure it out, and I will get you the right answer."

NOTE *Techno-babble* is the use of (often nonsensical) jargon and technical terms to intimidate and silence a challenge to a technical issue.

A computer tech must bring *integrity* to the job, just like any other service professional. You should treat anything said to you and anything you see as a personal confidence, not to be repeated to customers, coworkers, or bosses. Here's Mike's Rule of Confidentiality: "Unless it's a felony or an imminent

physical danger, you didn't see nothin'." You'll learn more about dealing with prohibited content in Chapter 27, "Securing Computers."

There is an exception to this rule. Sometimes you need to separate paying customers from in-house users. A paying customer is someone who doesn't work for your company and is paying for your services. An in-house user is someone who works for the same company you work for and is not directly paying for your services. It's often your job (but not always) to police in-house IT policies. Here's a great example. If you are at a customer's site and you see a sticky note with a password on a user's monitor, you say nothing. If you are in-house and you see the same thing, you probably need to speak to the user about the dangers of exposing passwords.

You have a lot of power when you sit in front of someone's computer. You can readily read private e-mail, discover Web sites surfed, and more. With a click of the Start button, you can know the last five programs the user ran, including Word and Solitaire, and the last few documents the user worked on. Don't do this; you really don't want to know. Plus, if you are caught violating a customer's privacy, you not only will lose credibility and respect, but you could also lose your job. *You need to deal appropriately with customers' confidential and private materials.* This includes files on the computer, items on a physical desktop, and even pages sitting in a printer tray.

Every user's password represents a potential danger spot for techs. We're constantly rebooting computers, accessing protected data, and performing other jobs that require passwords. The rule here is to *avoid learning other folks' passwords at all costs* (see Figure 1-3). If you know a password to access a mission-critical machine and that machine ends up compromised or with data missing, who might be blamed? You, that's who, so avoid learning passwords! If you only need a password once, let the user type it in for you. If you anticipate accessing something multiple times (the more usual situation), ask the user to change the password temporarily.

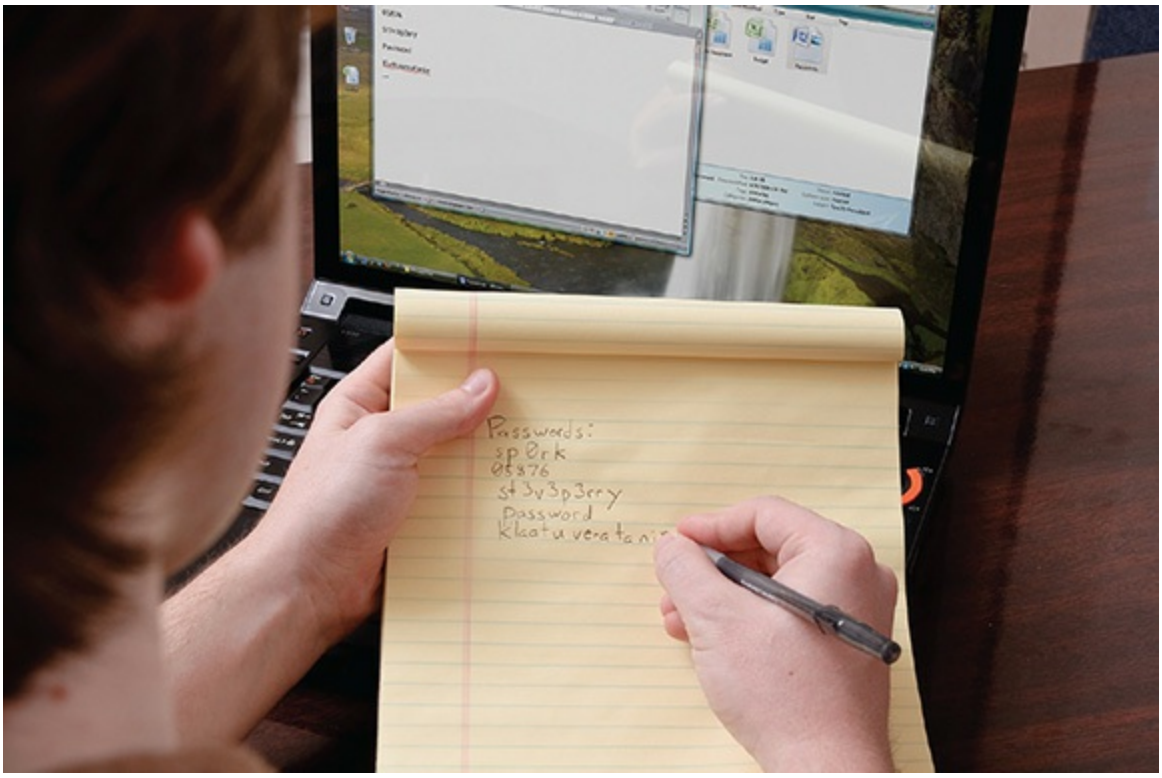

Figure 1-3 Don’t do this!

It’s funny, but people assume ownership of things they use at work. John in accounting doesn’t call the computer he uses anything but “my PC.” The phone on Susie’s desk isn’t the company phone, it’s “Susie’s phone.” Regardless of the logic or illogic involved with this sense of ownership, a tech needs to respect that feeling. You’ll never go wrong if you follow the *Ethic of Reciprocity*, also known as the *Golden Rule*: “Do unto others as you would have them do unto you.” In a tech’s life, this can translate as “Treat people’s things as you would have other people treat yours.” Don’t use or touch anything—keyboard, printer, laptop, monitor, mouse, phone, pen, paper, or cube toy—without first asking permission. Follow this rule at all times, even when the customer isn’t looking.

Dependability/Responsibility

Dependability and responsibility are another pair of traits that, while they don’t mean the same thing, often go together. A dependable person performs agreed-upon actions. A responsible person is answerable for her actions. Again, the freedom of the typical IT person’s job makes dependability and

responsibility utterly critical.

Dependable techs show up for job appointments and show up on time. Failure to show up for an appointment not only inconveniences the customer, but also can cost your customer a lot of money in lost time and productivity. So, *be on time.*

If you or your company makes an appointment for you, show up. Be there. Don't let simple problems (such as bad traffic) prevent you from showing up on time. Take some time to prepare. Figure out traffic times. Figure out if preceding appointments will cause a problem, and check for traffic. There is a popular old saying in the United States, "Five minutes early is on time, and on time is late." Sometimes events take place that prevent you from being on time. *If late, contact the customer immediately* and give him or her your best estimate of when you will arrive. A simple apology wouldn't hurt, either.

Responsibility is a tricky subject for IT folks. Certainly you should be responsible for your actions, but the stakes are high when critical data and expensive equipment are at risk. Before you work on a computer, always ask the customer if there are up-to-date backups of the data. If there aren't, offer to make backups for the customer, even if this incurs an extra charge for the customer. If the customer chooses not to make a backup, make sure he or she understands, very clearly, the risk to the data on the system you are about to repair.

NOTE Most computer repair companies require a signed Authorization of Work or Work Authorization form to document the company name, billing information, date, scope of work, and that sort of thing. Even if you do your own repairs, these forms can save you from angst and from litigation. You can create your own or do an Internet search for examples.

Sensitivity

Sensitivity is the ability to appreciate another's feeling and emotions. Sensitivity requires observing others closely, taking time to appreciate their feelings, and acting in such a way that makes them feel comfortable. I've

rarely felt that technicians I've met were good at sensitivity. The vast majority of nerds I know, including myself, tend to be self-centered and unaware of what's going on around them. Let me give you a few tips I've learned along the way.

Understand that the customer is paying for your time and skills. Also understand that your presence invariably means something is wrong or broken, and few things make users more upset than broken computers. When you are "on the clock," you need to show possibly very upset customers that you are giving their problem your full attention. To do this, you need to avoid distractions. If you get a personal call, let it roll over to voicemail. If you get a work-related call, politely excuse yourself, walk away for privacy, and keep the call brief. Never talk to coworkers while interacting with customers. Never speak badly of a customer; you never know where you'll run into them next.

Last, *be culturally sensitive.* We live in a diverse world of races, religions, etiquettes, and traditions. If a customer's religious holiday conflicts with your work schedule, the customer wins. If the customer wants you to take off your shoes, take them off. If the customer wants you to wear a hat, wear one. *Use appropriate professional titles, when applicable.* If a customer's title is "Doctor," for example, use the title even if you don't recognize the field of medicine. When in doubt, always ask the customer for guidance.

Effective Communication

When you deal with users, managers, and owners who are frustrated and upset because a computer or network is down and they can't work, your job requires you to take on the roles of detective and psychologist. Talking with frazzled and confused people and getting answers to questions about how the personal computing device got into the state it's in takes skill. Communicating clearly and effectively is important.

This section explores techniques for effective communication. It starts with assertive communication and then looks at issues involving respect. We'll examine methods for eliciting useful answers in a timely fashion. The section finishes with a discussion about managing expectations and professional follow-up actions.

Assertive Communication

In many cases, a computer problem results from user error or neglect. As a technician, you must show users the error of their ways without creating anger or conflict. You do this by using assertive communication. *Assertive communication* isn't pushy or bossy, but it's also not the language of a pushover. Assertive communication first requires you to show the other person that you understand and appreciate the importance of his feelings. Use statements such as "I know how frustrating it feels to lose data," or "I understand how infuriating it is when the network goes out and you can't get your job done." Statements like these cool off the situation and let customers know you are on their side. Avoid using the word "you," as it can sound accusatory.

The second part of assertive communication is making sure you state the problem clearly without accusing the user directly. Here's an example: "Help me understand how the network cable keeps getting unplugged during your lunch hour." Last, tell the user what you need to prevent this error in the future. "Please call me whenever you hear that buzzing sound," or "Please check the company's approved software list before installing anything." Always use "I" and "me," and never make judgments. "I can't promise the keyboard will work well if it's always getting dirty" is much better than "Stop eating cookies over the keyboard, you slob!"

Respectful Communication

Generally, IT folks support the people doing a company's main business. You are there to serve their needs and, all things being equal, to do so at their convenience, not yours.

You don't do the user's job, but you should *respect* that job and person as an essential cog in the organization. Communicate with users the way you would like them to communicate with you, were the roles reversed. Again, this follows the Ethic of Reciprocity.

Don't assume the world stops the moment you walk in the door and that you may immediately interrupt a customer's work to do yours. Although most customers are thrilled and motivated to help you the moment you arrive, this may not always be the case. Ask the magic question, "May I start working on the problem now?" Give customers a chance to wrap up, shut

down, or do anything else necessary to finish their business and make it safe for you to do yours.

Engage the user with the standard rules of civil conversation. *Actively listen*. Avoid interrupting the customer as he or she describes a problem; *just listen and take notes.* You might hear something that leads to resolving the problem. Rephrase and repeat the problems back to the customer to verify you understand the issue ("So the computer is locking up three times a day?"). Use an even, nonaccusatory tone, and although it's okay to try to explain a problem if the user asks, *never condescend and never argue with a customer.*

Maintain a positive attitude in the face of adversity. Don't get defensive if you can't figure something out quickly and the user starts hassling you. Remember that an angry customer isn't really angry with you—he's just frustrated—so don't take his anger personally. Instead, take it in stride; smile, *project confidence,* and assure him that computer troubleshooting sometimes takes a while.

Avoid distractions that take your focus away from the user and his or her computer problem. Things that break your concentration slow down the troubleshooting process immensely. Plus, customers will feel insulted if you start texting or talking to coworkers while interacting with the customer. You're not being paid to socialize, so turn those cell phones to vibrate. That's why the technogods created voicemail. Avoid personal interruptions or personal calls. Never take any call except one that is potentially urgent. If a call is potentially urgent, explain the urgency to the customer, step away, and deal with the call as quickly as possible.

Also, avoid accessing social media sites while on the job. Checking Facebook or tweeting while your customer waits for his computer to get fixed is rude. And definitely never disclose experiences with customers via social media outlets.

Try This! Apply the Ethic of Reciprocity

The Ethic of Reciprocity appears in almost every religion on the planet, with ver-sions attributed to Confucius, Jesus, Moses, and Mohammed, among others. Just for practice, try the Ethic of Reciprocity out in nontechnical situations, such as when buying something from the corner store or grocery. Consciously analyze how the clerk behind the counter

would want a customer to interact with him or her. Now put yourself in the clerk's shoes. How would you want a customer to commu-nicate with you? Act accordingly!

If you discover that the user caused the problem, either through ignorance or by accident, don't dismiss the customer's problem, but avoid being judgmental or insulting about the cause. We all screw up sometimes, and these kinds of mistakes are your job security. *You get paid because people make mistakes and machines break.* Chances are you'll be back at that workstation six months or a year later, fixing something else. By becoming the user's advocate and go-to person, you create a better work environment. If a mistaken action caused the problem, explain in a positive and supportive way how to do the task correctly, and then have the user go through the process while you are there to reinforce what you said.

Getting Answers

Your job as a tech is to get the computer fixed, and the best way to start that process is to determine what the computer is doing or not doing. You must start by talking to the customer. Allow the customer to explain the problem fully while you record the information.

Although each person is different, most users with a malfunctioning computer or peripheral will be distraught and perhaps defensive about the problem. There are methods for dealing with difficult customers or situations. You need to ask the right questions *and* listen to the customer's answers. Then ask the proper follow-up questions with the goal of *getting answers* that will help you troubleshoot the problem.

Always avoid accusatory questions, because they won't help you in the least (see Figure 1-4). "What did you do?" generally gets a confused or defensive "Nothing" in reply, which doesn't get you closer to solving the problem. First, ask questions that help clarify customer statements. Repeat what you think is the problem after you've listened all the way through the user's story.

Figure 1-4 Never accuse!

Follow up with fact-seeking questions. “When did it last work?” “Has it ever worked in this way?” “Has any software changed recently?” “Has any new hardware been added?” Ask open-ended questions to narrow the scope of the problem (“Which applications are running when the computer locks up?”).

By keeping your questions friendly and factual, you show users that you won’t accuse them or judge their actions (see Figure 1-5). You also show them that you’re there to help them. After the initial tension drops away, you’ll often get more information: for instance, a recitation of something the user might have tried or changed. These clues can help lead to a quick resolution of the problem.

Figure 1-5 Keeping it friendly

Remember that you may know all about computer technology, but the user probably does not. This means a user will often use vague and/or incorrect terms to describe a particular computer component or function. That's just the way it works, so don't bother to correct the user. Wherever possible, use proper language and avoid jargon, acronyms, and slang when applicable. They simply confuse the already upset user and can make you sound like you're talking down to the user. Just ask direct, factual questions in a friendly tone, using simple, non-jargon language to zero in on what the user was trying to accomplish and what happened when things went wrong. Use visual aids when possible. Point at the machine or go to a working computer to have the user show what went wrong or what she did or tried to do.

People do usually want to get a handle on what you are doing—in a simplified way. You don't want to overwhelm them, but don't be afraid to use simple analogies or concepts to give them an idea of what is happening. If you have the time (and the skills), use drawings, equipment, and other visual aids to make technical concepts more clear. If a customer is a closet tech and is really digging for answers—to the point that it's affecting your ability to do your job—compliment her initiative and then direct her to outside training opportunities. Better yet, tell her where she can get a copy of

this book!

Beyond basic manners, never assume that just because you are comfortable with friendly or casual behavior, the customer will be too. Even an apparently casual user will expect you to behave with professional decorum. On the flip side, don't allow a user to put you in an awkward or even potentially dangerous or illegal situation. Never do work outside the scope of your assigned duties without the prior approval of your supervisor (when possible in such cases, try to direct users to someone who *can* help them). You are not a babysitter; never volunteer to "watch the kids" while the customer leaves the job site or tolerate a potentially unsafe situation if a customer isn't properly supervising a child. Concentrate on doing your job safely and efficiently, and maintain professional integrity.

Expectations and Follow-up

Users are terrified when their computers and networks go down so hard that they need to call in a professional. Odds are good that they've left critical, or at least important, data on the computer. Odds are equally good they need this computer to work to do their job. When they're ready to lay down money for a professional, they're expecting you to make their system exactly the way it was before it broke. Hopefully you can do exactly that for them, but you also must deal with their expectations and let them know what to expect.

Equally, you should give your customers some follow-up after the job is finished. We've already covered data backups and Authorization of Work forms (and those are very important), but you need to keep the customer's needs in mind. You also want to keep the customer thinking about you, should they need more help in the future. Here are a few items you should consider.

Timeline

If you can give the customer a best guess as to how long the repair will take, you'll be a hero. Don't be afraid to hold off on your time frame prediction until you've diagnosed the machine. If you truly don't have a feel for the time involved, tell the customer that and then tell him or her what you'll need to know before you can make the prediction.

Set and meet expectations and the timeline and communicate status with

the customer. Stick to the timeline. If you finish more quickly, great! People love a job that goes faster than predicted. If you're moving past the predicted time frame, contact the customer and tell him or her as soon as possible. Let him or her know what's happened, explain why you need more time, and give the customer a new time frame. The biggest secret here is to keep in communication with the customer on any change in status. People understand delays—they take place in our lives daily. People resent not knowing why a delay is occurring, especially when a precious computer is at stake.

Options

Many times with a computer issue, you can fix the problem and avoid a similar problem in the future in several ways. These options boil down to money. If applicable, offer different repair/replacement options and let the customer decide which route to take.

Route A might replace a faulty component with an upgraded component and a backup in case the new component fails in the future. Route B might replace the faulty device with an upgraded device. Route C might do an even device swap. Provide options and let the customer decide.

Documentation

At the completion of work, provide proper documentation of the services provided. Describe the problem, including the time and day you started work, the solution (again including the time and day the work ended), the number of hours you worked, and a list of all parts you replaced. If the customer owns the replaced parts, offer them to the customer (this is especially true if you replace any storage media). This documentation may or may not include your charges.

Follow-up

Follow up with a customer/user at a later date to verify satisfaction. This can be simple follow-up, usually just a phone call, to confirm that the customer is happy with your work. This gives the customer a chance to detail any special issues that may have arisen, and it also adds that final extra touch that ensures he or she will call you again when encountering a technical problem.

Be Prepared!

Effective communication with your customer enables you to *start* the troubleshooting process, getting details about the problem and clues about things that happened around the same time. To continue troubleshooting, though, you need to be adept at handling computing devices. That starts with knowing how to handle computer components safely and how to use the tools of a tech. You also need a very clear troubleshooting methodology to guide your efforts. Let's look at these issues.

Electrostatic Discharge (ESD)

All computing devices use electricity. As long as the electricity runs properly through the circuits and wires as designed, all is good. There are times when electricity improperly jumps from one place to another in ways that cause damage, an *electromagnetic pulse* (*EMP*). EMP shows up in many ways. Lightning is a form of EMP. Lightning hitting your electrical equipment certainly makes a bad day! Nuclear detonations also create a massive EMP burst (yikes!), but the EMP of most concern to techs is *electrostatic discharge* (*ESD*).

ESD simply means the passage of a static electrical charge from one item to another. Have you ever rubbed a balloon against your shirt, making the balloon stick to you? That's a classic example of static electricity. When that static charge discharges, you may not notice it happening—although on a cool, dry day, I've been shocked so hard by touching a doorknob that I could see a big, blue spark! I've never heard of a human being getting anything worse than a rather nasty shock from ESD, but I can't say the same thing about computers. ESD will destroy the sensitive parts of any computing device, so it is essential that you take steps to avoid ESD when working on a PC or other computing device.

NOTE All computing devices are well protected against ESD on the outside. Unless you take a screwdriver or pry tool and open up a PC or other

computing device, you don’t need to concern yourself with ESD.

Antistatic Tools

ESD only takes place when two objects that store different amounts (the hip electrical term to use is *potential*) of static electricity come in contact. The secret to avoiding ESD is to keep you and the parts of the computer you touch at the same electrical potential, otherwise known as grounding yourself to the computing device. You can accomplish this by connecting yourself to the computer via a handy little device called an *antistatic wrist strap*, or *ESD strap*. This simple device consists of a wire that connects on one end to an alligator clip and on the other end to a small metal plate that secures to your wrist with an elastic strap. You snap the alligator clip onto any handy metal part of the computer and place the wrist strap on either wrist. Figure 1-6 shows a typical antistatic wrist strap in use.

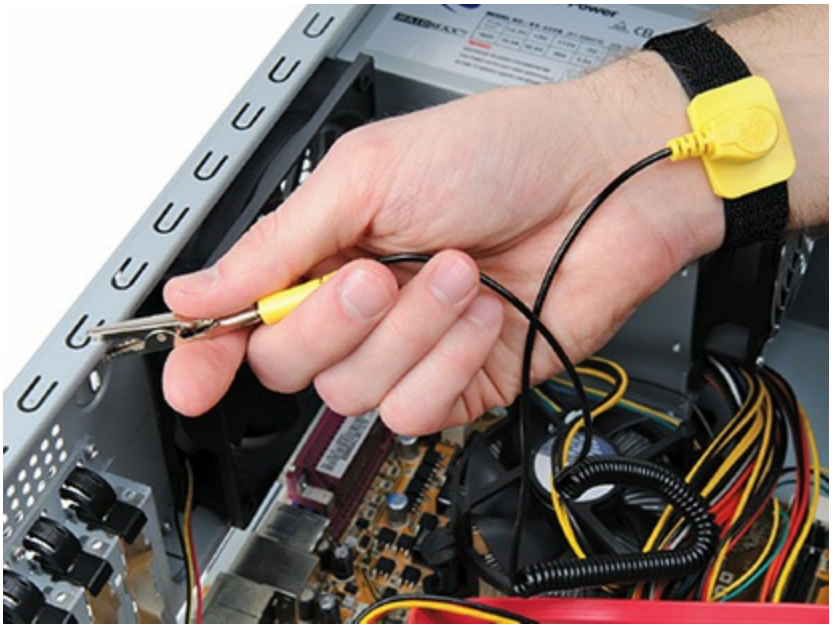

Figure 1-6 Antistatic wrist strap in use

EXAM TIP Static electricity, and therefore the risk of ESD, is much more

prevalent in dry, cool environments.

Antistatic wrist straps are standard equipment for anyone working on a computing device, but other tools might also come in handy. One of the big issues when working with a computer occurs if you find yourself pulling out parts from the computer and setting them aside. The moment you take a piece out of the computer, it no longer has contact with the systems and may pick up static from other sources. Techs use antistatic mats to eliminate this risk. An *antistatic mat*—or *ESD mat*—acts as a point of common potential; it's typical to purchase a combination antistatic wrist strap and mat that all connect to keep you, the computer, and any loose components at the same electrical potential (see Figure 1-7).

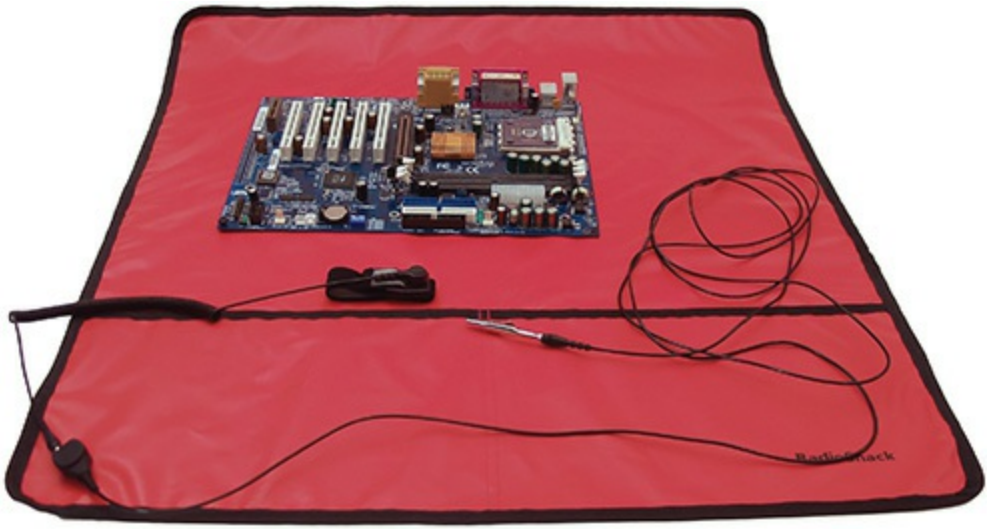

Figure 1-7 Antistatic wrist strap and mat combination

NOTE Make sure the metal plate on the antistatic wrist strap touches the skin of your wrist. Don't put it on over the sleeve of a long-sleeved shirt.

Antistatic wrist straps and mats use tiny *resistors*—devices that stop or *resist* the flow of electricity—to prevent a static charge from racing through the device. These resistors can fail over time, so it's always a good idea to

read the documentation that comes with your antistatic tools to see how to test those small resistors properly.

EXAM TIP Always put components *in* an antistatic bag, not on the bag.

Any electrical component not in a computer case needs to be stored in an *antistatic bag*, a specially designed bag that sheds whatever static electricity you have when you touch it, thus preventing any damage to components stored within (see Figure 1-8). Almost all components come in an antistatic bag when purchased. Experienced techs never throw these bags away, as you never know when you'll want to pull a part out and place it on a shelf for a while.

Figure 1-8 Antistatic bag

Although having an antistatic wrist strap with you at all times would be ideal, the reality is that from time to time you'll find yourself in a situation where you lack the proper antistatic tools. This shouldn't keep you from working on the computer—if you're careful! Before working on a computer in such a situation, take a moment to touch the power supply every once in a while as you work—I'll show you where it is in Chapter 2, "The Visible Computer"—to keep yourself at the same electrical potential as the computer. Although this isn't as good as a wrist strap, this *self-grounding* is better than nothing at all.

Use these tools for proper component handling and storage: ESD straps, ESD mats, antistatic bags, and self-grounding.

Try This! Antistatic Protection Devices

In some circumstances, an antistatic wrist strap could get in the way. Manufacturers have developed some alternatives to the wrist strap, so try this:

1. Take a field trip to a local computer or electronics store.
2. Check out their selection of antistatic devices. Can you find anything other than wrist straps or mats?
3. Do a Web search for "static control products." Can you find anything other than wrist straps or mats?
4. Report what options you can find for protecting your equipment from ESD. Weigh the pros and cons and decide what you would use in various situations.

The last issue when it comes to preventing ESD is that never-ending question—should you work with the computing device plugged in or unplugged? The answer is simple: Do you really want to be physically connected to a computer that is plugged into an electrical outlet? Granted, the chances of electrocution are slim, but why take the risk?

EXAM TIP Always disconnect power before repairing a personal computing device.

Removing the power applies also when working on portable computers. Disconnect both from the wall outlet and remove the battery. With mobile devices such as tablets and smartphones, this creates an issue because the battery is inside the case. Chapter 25, "Care and Feeding of Mobile Devices," covers the special skills needed for working on mobile devices.

Electromagnetic Interference (EMI)

A magnetic field interfering with electronics is *electromagnetic interference* (*EMI*). EMI isn't nearly as dangerous as ESD, but it can cause permanent damage to some components and erase data on some storage devices. You can prevent EMI by keeping magnets away from computer equipment. Certain components are particularly susceptible to EMI, especially storage devices like hard drives.

The biggest problem with EMI is that we often use magnets without even knowing we are doing so. Any device with an electrical motor has a magnet. Many telephones have magnets. Power bricks for laptops and speakers also have magnets. Keep them away!

Radio Frequency Interference (RFI)

Do you ever hear strange noises on your speakers even though you aren't playing any sounds? Do you ever get strange noises on your cell phone? If so, you've probably run into *radio frequency interference* (*RFI*). Many devices emit radio waves:

- Cell phones
- Wireless network cards
- Cordless phones
- Baby monitors
- Microwave ovens

In general, the radio waves that these devices emit are very weak, and almost all electronic devices are shielded to prevent RFI. A few devices,

speakers in particular, are susceptible to RFI. RFI will never cause any damage, but it can be incredibly irritating. The best way to prevent RFI is to keep radio-emitting devices as far away as possible from other electronics.

RFI becomes a big problem when two devices share the same frequencies. Cordless phones, baby monitors, and many wireless networks share the same range of frequencies. They sometimes interfere with each other, causing poor signals or even blocking signals completely. These devices need to be tuned to avoid stomping on each other's frequencies. In Chapter 20, "Wireless Networking," you'll see how to tune a wireless network to prevent RFI.

NOTE Computer gear manufacturers package their products in a variety of ways to shield against accidental damage, whether that's physical damage, ESD, EMI, or RFI. The typical pink translucent computer bag is coated with a film that prevents the bag from producing static electricity and mildly protects the contents against physical contact (and thus damage). The two types of metal bags offer shielding against EMI and RFI as well as ESD. These are the silvery bags (such as in Figure 1-8) you'll see hard drives packed in, for example, and the black-and-silver woven bags you'll sometimes see.

Physical Tools

The basic *tech toolkit* consists of a Phillips-head screwdriver and not much else—seriously—but a half-dozen tools round out a fully functional toolkit. Most kits have a star-headed Torx wrench, a nut driver or two, a pair of plastic tweezers, a little grabber tool (the technical term is *parts retriever*), a hemostat, and both Phillips-head and flat-head screwdrivers (see Figure 1-9).

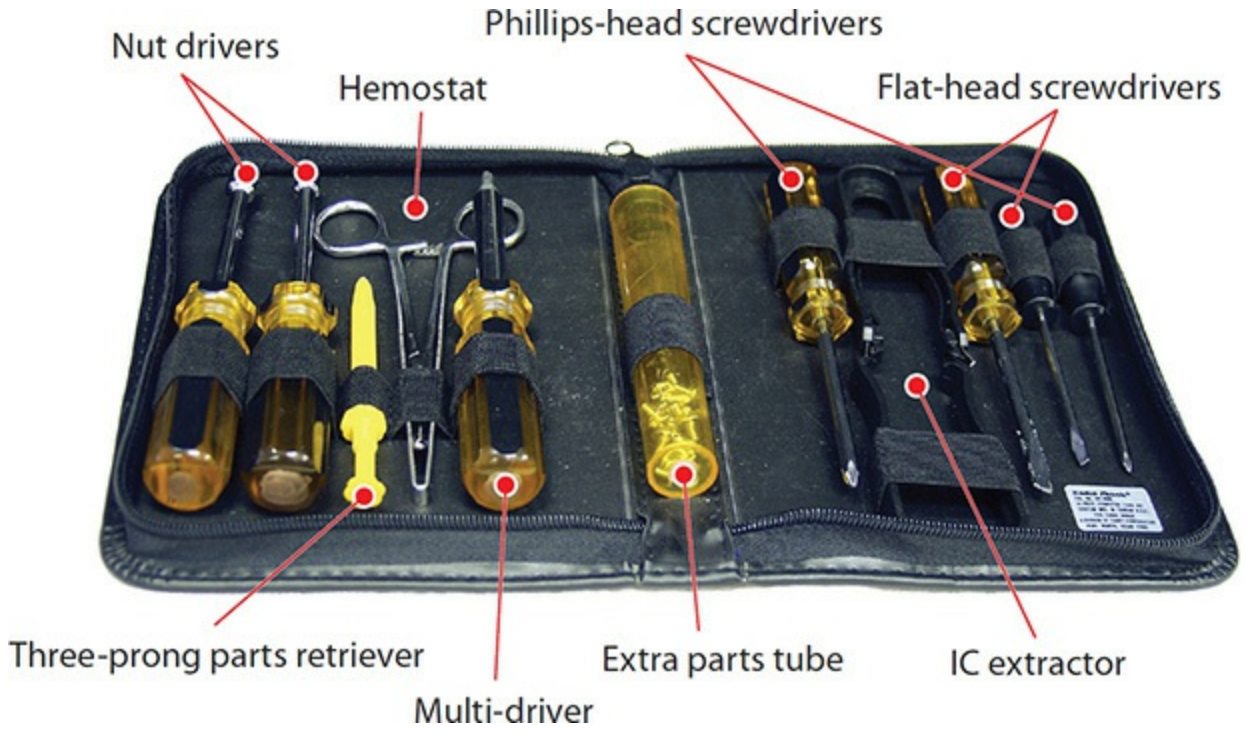

Figure 1-9 Typical technician toolkit

I'll add a few more tools to this toolkit as the book progresses that you'll want for a not-so-basic toolkit. Those more advanced tools will be introduced as your knowledge grows.

You already own another great tool, the camera in your smartphone or tablet. It's amazing how handy it is to photograph screw locations, cable connections, or other conditions so that you can later retrieve those images when you reinstall something.

A lot of techs throw in an extension magnet to grab hard-to-reach bits that drop into cases (an exception to the "no magnets" rule). Many also add a magnifying glass and a flashlight for those hard-to-read numbers and text on the printed circuit boards (PCBs) that make up a large percentage of devices inside the system unit. Contrary to what you might think, techs rarely need a hammer.

Mobile devices such as tablets and smartphones require more complex kits that include specialized tools, such as prying tools (called *spudgers*—isn't that a great word?). There are many excellent toolkits available for purchase; I recommend the toolkits sold by iFixit (www.ifixit.com) and use one myself (Figure 1-10). These kits are inexpensive and reliable, plus iFixit has hundreds of free videos that walk you through many scenarios using the kits.

Figure 1-10 Author's go-to iFixit toolkit (several of the implements on the right side are types of spudger)

Personal Safety

IT techs live in a dangerous world. We're in constant danger of tripping, hurting our backs, and getting burned by hot components. You also need to keep in mind what you wear (in a safety sense). Let's take a moment to discuss these *personal safety* issues and what to do about them.

CAUTION When thinking about safety, maintain compliance with government regulations. You may be required to wear certain protective gear or take extra precautions while in the workplace. Make sure you also follow any environmental rules for the disposal of old parts, especially with things like CRT monitors, batteries, and toner cartridges, which may contain hazardous or toxic materials. Check with your employer or your local government's Web site for more information.

If you don't stay organized, hardware technology will take over your life.

Figure 1-11 shows a corner of my office, a painful example of cable "kludge."

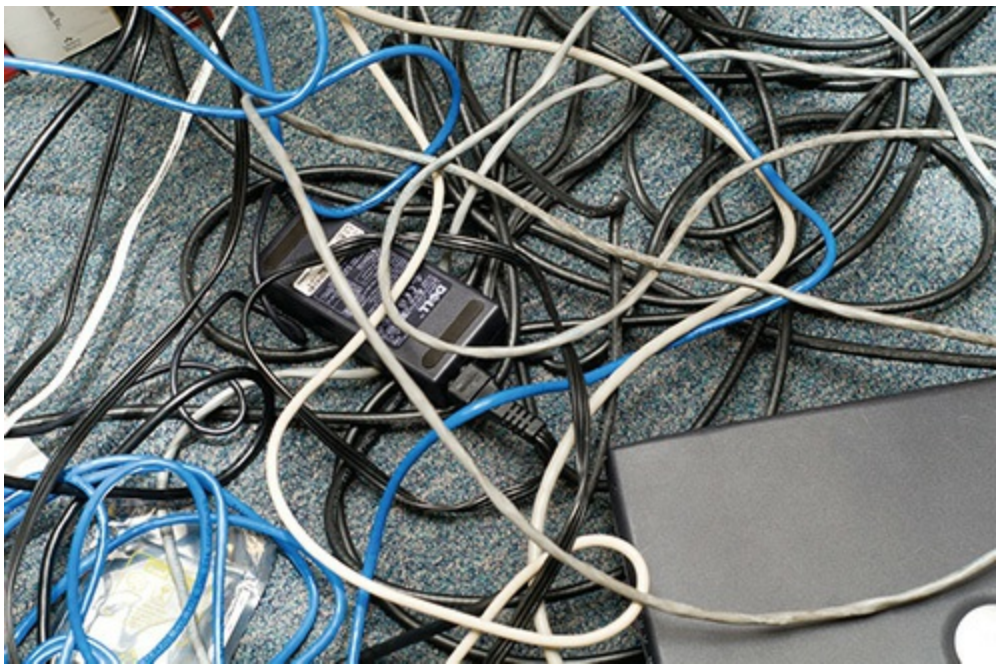

Figure 1-11 Mike's cable kludge

Cable messes such as these are dangerous tripping hazards. While I may allow a mess like this in my home office, all cables in a business environment are carefully tucked away behind computer cases, run into walls, or placed under cable runners. If you see a cable that is an obvious tripping hazard, contact the person in charge of the building to take care of it immediately. The results of ignoring such hazards can be catastrophic (see Figure 1-12). Use proper cable management to avoid these dangers.

Figure 1-12 What a strange, bad trip it's been.

Another personal safety issue is heavy boxes. Computers, printers, monitors—everything we use—all seem to come to us in heavy boxes. Use proper lifting techniques. Remember never to lift with your back; lift with your legs, and always use a hand truck if available. Pay attention to weight limitations on the devices you use to move anything heavy. You are never paid enough to risk your own health.

You also need to watch out for hot components. It's hard to burn yourself unless you open up a computer, printer, or monitor. First, watch for anything with a cooling fan like the one shown in Figure 1-13. If you see a cooling fan, odds are good that something is hot enough to burn you—such as the metal *cooling fins* below the fan. Also look for labels or stickers warning about hot components. Last, when in doubt, move your hand over components as if you were checking the heat on a stove.

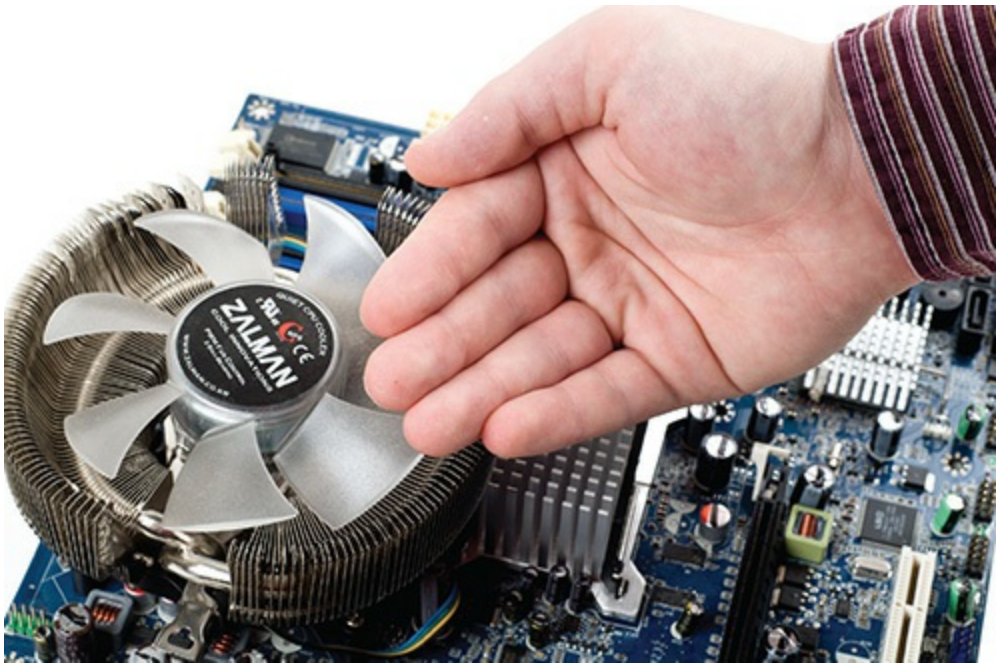

Figure 1-13 Checking for hot cooling fins

Disconnect a computer from its electrical source before you work on it, if possible. In the rare event where you need to work on a live system, take caution. Provide electrical fire safety equipment in rooms or locations that have a fire risk, such as server rooms. All those electronics and all that juice make a dangerous combination in those rare circumstances in which bad things happen. Keep properly rated (Class C) fire extinguishers handy.

EXAM TIP When you build out a computer space, such as a server closet (the room that has a lot of important computers in it), use standard carpentry safety techniques. Wear an air filter mask when cutting drywall, for example. Wear safety goggles when using power tools.

Finally, remove any jewelry or loose-hanging clothing before working on a computer. If you have long hair, you might consider tying it back in a ponytail. You don't want anything getting caught in a fan or stuck on a component. This can save you and your components a lot of pain.

Troubleshooting Methodology

An effective *troubleshooting methodology* follows a set of steps to diagnose and fix a computer. Troubleshooting methodology includes talking to users to determine how and when the problem took place, determining a cause, testing, verification, and documentation. Techs use a number of good troubleshooting methodologies. Luckily for those taking the CompTIA A+ 220-1001 certification exam, CompTIA clearly defines their vision of troubleshooting methodology:

5.1 Given a scenario, use the best practice methodology to resolve problems

1. Identify the problem
   - Question the user and identify user changes to computer and perform backups before making changes
   - Inquire regarding environmental or infrastructure changes
   - Review system and application logs
2. Establish a theory of probable cause (question the obvious)
   - If necessary, conduct external or internal research based on symptoms
3. Test the theory to determine cause
   - Once the theory is confirmed, determine the next steps to resolve problem
   - If theory is not confirmed re-establish new theory or escalate
4. Establish a plan of action to resolve the problem and implement the solution
5. Verify full system functionality and, if applicable, implement preventive measures
6. Document findings, actions, and outcomes

Identify the Problem

There's a reason you're standing in front of a computer to repair it: something happened that the user of the computer has identified as "not good" and that's why you're here. First, you need to *identify the problem* by talking to the user. Get the user to show you what's not good. Is it an error code? Is something not accessible? Is a device not responding?

Then ask the user that classic tech question (remember your communication skills here!): “Has anything recently changed on the computer that might have made this problem appear?” What you’re really saying is: “Have you messed with the computer? Did you install some evil program? Did you shove a USB drive in so hard that you broke the connection?” Of course, you never say these things; simply ask nicely without accusing so the user can help you troubleshoot the problem (see Figure 1-14).

Figure 1-14 Tech asking nicely

Ask also if any changes have happened in the environment around the workstation. Check for any infrastructure changes that might cause problems. If you can access them, review system and application logs for clues about faulty software.

In most troubleshooting situations, it’s important to back up critical files before making changes to a system. To some extent, this is a matter of proper ongoing maintenance, but if some important bit of data disappears and you don’t have a backup, you know who the user will blame, don’t you? (We

cover backup options in detail in Chapter 14, “Maintaining and Optimizing Operating Systems.”)

EXAM TIP The CompTIA A+ certification exams assume that all techs should back up systems *every time* before working on them, even though that’s not how it works in the real world.

Establish a Theory of Probable Cause (Question the Obvious)

Now it’s time to analyze the issue and come up with a theory as to what is wrong, a *theory of probable cause.* Personally, I prefer the word “guess” at this point because very few errors are so obvious that you’ll know what to do. Fall back on your knowledge of the computing process to localize the issue based on the symptoms. Keep your guesses…err…theories…simple. One of the great problems for techs is their desire to overlook the obvious problems in their desire to dig into the system (see Figure 1-15).

Figure 1-15 Ford the Tech misses the obvious.

NOTE Chapter 2, "The Visible Computer," walks you through the computing process in some detail, showing how all the parts interact to make magic happen. The combination of a solid troubleshooting theory and a

fundamental understanding of the computing process is the core knowledge for techs for fixing things.

Research In many situations, you'll need to access other resources to root out the most probable cause of the problem. If necessary, therefore, you should conduct external or internal research based on the symptoms.

Use the Internet for external research. With the Internet quite literally at the fingertips of anyone with access to a smartphone or tablet, a short search online can result in swift answers to tech problems. If the customer's computer displays an error message, for example, put the whole error message into a search engine.

Internal research means asking other techs on-site for help. It means checking company records regarding a particular machine (for example, checking a problem-tracking database where previous issues have been recorded). This kind of search will reveal any known problems with the machine or with the user's actions.

Outside the Case Take a moment to look for clues before you open up the case. Most importantly, use all your senses in the process.

What do you see? Is a connector mangled or a plastic part clearly damaged? Even if that connector or part works fine, the physical abuse could provide extra information. If the user can't connect to a network, check the cable. Was something rolled over it that could have broken the thin internal wires? Is that a jelly smear near the jammed optical drive door? (No pun intended, really!) A visual examination of the external computer is important.

When you put your hand on the system unit (that's the case that houses all the computer parts), does it feel hot? Can you feel or hear the vibrations of the fans? If not, that would be a clue to an overheating or overheated computer. Modern computers can run when overly hot, but generally run very sluggishly.

If you spend a moment listening to the computer, you might get some clues to problem sources. A properly running computer doesn't make a lot of sound, just a regular hum from the spinning fans. If you hear clicking or grinding sounds, that's a very bad sign and a very important clue! We'll cover data storage devices—the usual cause of clicking and grinding sounds—in detail in Chapters 8 and 9.

Finally, don't forget your nose. If you smell the unmistakable odor of

ozone, you know that's the smell electronic components give off when they cook or are simply running much too hot.

Test the Theory to Determine Cause

Okay, so you've decided on a theory that makes sense. It's time to *test the theory* to see if it fixes the problem. A challenge to fixing a computer is that the theory and the fix pretty much prove themselves at the same time. In many cases, testing your theory does nothing more than verify that something is broken. If that's the case, then replace the broken part.

If your theory doesn't pan out, you should come up with a new theory and test it. (In CompTIA speak, if the theory is not confirmed, you need to re-establish a new theory.) If you verify and the fix lies within your skill set, excellent.

At this point, you need to check in with management to make certain you have permission to make necessary changes. Always consider corporate policies, procedures, and impacts before implementing changes. Having the boss walk in frowning while you're elbows-deep in a machine with the question "Who gave you permission?" can make for a bad day!

If you don't have the skills—or the permissions—to fix the issue, you need to *escalate* the problem.

Escalation is the process your company (or sometimes just you) goes through when you—the person assigned to repair a problem—are not able to get the job done. It's okay to escalate a problem because no one can fix every problem. All companies should have some form of escalation policy. It might mean calling your boss. It might mean filling out and sending some in-house form to another department. Escalation is sometimes a more casual process. You might want to start researching the problem online; you might want to refer to in-house documentation to see if this problem has appeared in the past. (See "Document Findings, Actions, and Outcomes" later in this chapter.) You may want to call a coworker to come check it out (see Figure 1-16).

Figure 1-16 Ford the Tech asks for help from Scott.

Establish a Plan of Action

At this point, you should have a good sense of the problem, including the scope and necessary permissions to do the job. You need to *establish a plan of action* to resolve the problem and implement the solution. Sometimes the plan requires a few steps before you can implement the solution. You might need additional resources such as known good replacement parts. A backup of user data should be part of the plan of action.

Verify and Prevent

Fantastic! Through either your careful work or escalation, you've solved the problem, or so you think. Remember two items here. First, even though *you* think the problem is fixed, you need to verify with the customer/user that it's fixed. Second, try to do something to prevent the problem from happening again in the future, if possible.

Verify Full System Functionality You need to *verify* full system

functionality to make sure the user is happy. Let's say a user can't print. You determine that the Print Spooler service is stalled due to a locked-up laser printer. You reset the printer and the jobs all start printing. Job done, right?

The best way to verify full system functionality is to have the user do whatever she needs to do on the repaired system for a few minutes while you watch. Any minor errors will quickly become apparent, and you might learn some interesting aspects of how the user does her job. Knowing what your users do is critical for good techs to help them do their jobs better (see Figure 1-17).

Figure 1-17 Ford the Tech sticks around and watches.

If Applicable, Implement Preventive Measures A very smart tech once told me, "A truly good support tech's work goal should be to never have to get out of his chair." That's a pretty tall order, but it makes sense to me. Do whatever you can to prevent this problem from repeating. For some problems, there are obvious actions to take, such as making sure anti-

malware is installed so a computer doesn't get infected again. Sometimes there's no action to take at all: nothing can prevent a hard drive that decides to die. But you can take one more critical action in almost every case: education. Take advantage of the time with the user to informally train him about the problem. Show him the dangers of malware or tell him that sometimes hard drives just die. The more your users know, the less time you'll spend out of your chair.

Document Findings, Actions, and Outcomes

Based on his famous quote, "Those who cannot remember the past are condemned to repeat it," I think the philosopher George Santayana would have made a great technician. As a tech, the last step of every troubleshooting job should be to *document* your findings, actions, and outcomes. This documentation might be highly formalized in some organizations, or it might just be a few notes you jot down for your own use, but you must document! What was the problem? What did you do to fix it? What worked? What didn't? The best guide to use for documentation is: "What would I have liked to have known about this problem before I walked up to it?" Good documentation is the strongest sign of a good tech (see Figure 1-18).

Figure 1-18 Ford documents a successful fix.

Documenting problems helps you track the troubleshooting history of a computing device over time, enabling you to make longer-term determinations about retiring it or changing out more parts. If you and fellow techs fix a specific problem with Mary's laptop several times, for example, you might decide to swap out her whole system rather than fix it a fourth time.

Documenting helps fellow techs if they have to follow up on a task you didn't finish or troubleshoot a machine you've worked on previously. The reverse is also true. If you get a call about Frank's computer, for example,

and check the records to find other service calls on his computer, you might find that the fix for a particular problem is already documented. This is especially true for user-generated problems. Having documentation of what you did also means you don't have to rely on your memory when your coworker asks what you did to fix the weird problem with Jane's computer a year ago!

Documenting also comes into play when you or a user has an accident onsite. If your colleague Joe drops a monitor on his foot and breaks both the monitor and his foot, for example, you need to fill out an *incident report*, just as you would with any kind of accident: electrical, chemical, or physical. An incident report should detail what happened and where it happened. This helps your supervisors take the appropriate actions quickly and efficiently.

Chapter Review

Questions

1. Which of the following would be most appropriate for the workplace? (Select two.)
   - **A.** Clean, pressed khaki trousers
   - **B.** Clean, wrinkle-free T-shirt
   - **C.** Clean, wrinkle-free polo shirt
   - **D.** Clean, pressed jeans
2. While manning the help desk, you get a call from a distraught user who says she has a blank screen. What would be a useful follow-up question? (Select two.)
   - **A.** Is the computer turned on?
   - **B.** Is the monitor turned on?
   - **C.** Did you reboot?
   - **D.** What did you do?
3. At the very least, what tool should be in every technician's toolkit?
   - **A.** Pliers
   - **B.** Hammer

C. Straight-slot screwdriver

D. Phillips-head screwdriver

4. When is it appropriate to yell at a user?

A. When he screws up the second time

B. When he interrupts your troubleshooting

C. When he screws up the fifth time

D. Never

5. When troubleshooting a software problem on Phoebe's computer and listening to her describe the problem, you get a text from your boss. Which of the following is the most appropriate action for you to take?

A. Excuse yourself, walk out of the cube, and text your boss.

B. Pick up Phoebe's phone and dial your boss's number.

C. Wait until Phoebe finishes her description and then ask to use her phone to call your boss.

D. Wait until Phoebe finishes her description, run through any simple fixes, and then explain that you need to call your boss on your cell phone.

6. You are at a customer's workstation to install several software and hardware updates, a process that will take a while and require several reboots of the computer. What should you do about the password to the user's account?

A. Require the customer to sit with you throughout the process so she can type in her password each time.

B. Ask the user to write down her password for you to use.

C. Ask the user to change her password temporarily for you to use.

D. Call your supervisor.

7. Which of the following is a good practice after completing a troubleshooting call at someone's office?

A. Follow up with a call within a couple of days to make sure everything is going well with the fixed computer.

B. Make copies of any passwords you used at the site for future reference.

C. Document any particularly important people you met for future reference.

D. Do nothing. Your work is finished there.

8. Which tool helps you avoid accidental static discharge by keeping you at the same electrical potential as the computer on which you're working?

   A. Antistatic spray

   B. Antistatic bag

   C. Antistatic wrist strap

   D. Phillips-head screwdriver

9. Once you have ascertained the computer's problem and backed up the critical data, what should you do?

   A. Establish a theory of probable cause.

   B. Start fixing the machine.

   C. Question users more to find out how they caused the problem.

   D. Document.

10. What should you do after successfully repairing a machine?

    A. Do nothing; your job is done.

    B. Admonish the user for causing so much work for the IT department.

    C. Document your findings.

    D. Lock it down so the user can't cause the same problem again.

Answers

1. **A, C.** Khaki trousers and a polo shirt trump jeans and a T-shirt every time.
2. **A, B.** Go for the simple answer first. When faced with a blank screen, check to see if the computer and the monitor are turned on.
3. **D.** Every tech's toolkit should have a Phillips-head screwdriver, at the very least.
4. **D.** Don't get angry or yell at clients.

5. **D.** Focus on the customer and don’t use her things.
6. **C.** In this circumstance, asking for a temporary password is the right answer. Make sure the user changes her password back before you leave the site.
7. **A.** A simple follow-up builds goodwill and trust. This is a very important step to take after completing a job.
8. **C.** An antistatic wrist strap keeps you at the same electrical potential as the computer.
9. **A.** You should establish a theory of probable cause once you have ascertained the problem and backed up data.
10. **C.** At the end of a repair you should always document your findings.