CHAPTER 2

Operational Procedures

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
- Work with PCs safely using the proper tools

One of the interesting parts of teaching new techs is keeping up with the skills that get a tech a job and the issues that cause them to lose the jobs they get. To me, the number one reason techs fail to get or hold onto a job isn't lack of technical skill; it's lack of what CompTIA calls "operational procedures." Personally, I think a better name might be "life skills and basic safety," but it boils down to the same thing: nontechnical skills that technicians are famous for lacking.

I like to describe myself as a "nerd" and I consider it a compliment if you call me one. Nerds are smart and like to work with technology—these are the good aspects of nerd-dom. On the other hand, most people would 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. 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 dress, how to act, and how to communicate. 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.

Essentials

The Professional Tech

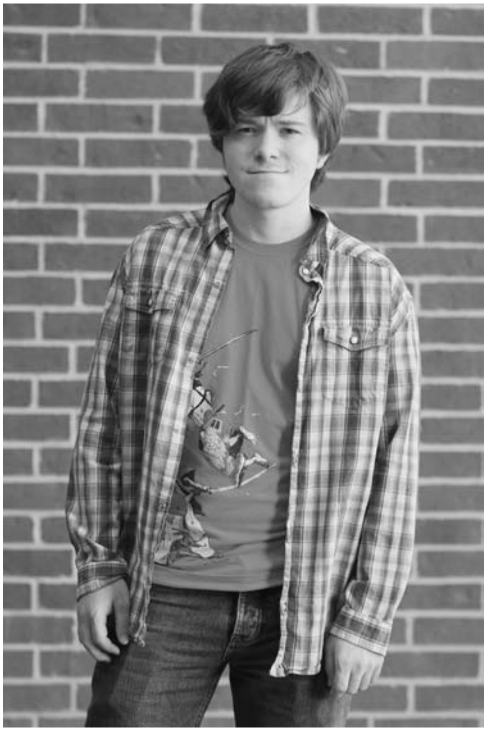
A professional tech displays professionalism, which might seem a little trite if it weren't absolutely true. The tech presents a professional appearance and follows a proper ethical code. I call the latter the Traits of a Tech. Let's take a look at these two areas in more detail.

Appearance

Americans live in a casual society, and I think that's great, because I prefer dressing casually. The problem with casual is that perhaps our society is becoming *too* casual. New techs sometimes fail to appreciate that customers 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. Take a look at Figure 2-1. This is our resident illustrator (among other job descriptions), Ford Pierson, casually dressed to hang with his buddies.

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 2-2 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.

Figure 2-1
Casual Ford



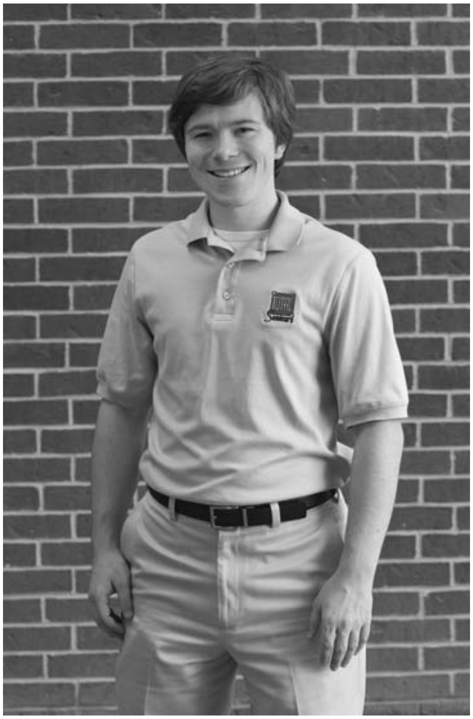


Figure 2-2
Professional Ford

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 did, 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.

The Traits of a Tech

When I was a Boy Scout in the United States, we learned something called The Boy Scout Creed, a list of traits that define the ethics of a Boy Scout. Even thought I haven't been a Boy Scout for a long time, I still have them 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/reliability, adaptability/versatility, 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 is a reflection of their skill. In your humble author’s opinion, there is no greater proof of a quality technician than the ability to 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. Anything said to you and anything you see, you should treat 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’.”

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, who is paying for your services. An in-house user is someone who works for the same company you do 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 post-it 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, not only will you lose credibility and respect, you could also lose your job.

Passwords are a big issue for techs. We have to reboot computers and access shares and other jobs that require passwords. The rule here is to *avoid learning other folks' passwords at all costs* (Figure 2-3). 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.

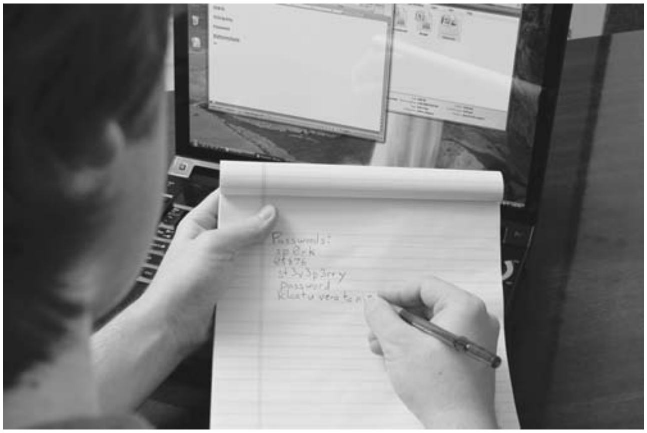


Figure 2-3
Don't do this!

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 responsible person is answerable for the acts she does. A dependable person can be counted on to perform those acts. Again, the freedom of the typical IT person's job makes dependability and responsibility utterly critical.

The single biggest dependability issue for an IT technician is to show up for job appointments and to show up on time. It seems to me we now live in a society where not showing up and not letting anyone know is normal. I call it the "Age of the Blow-off." We've all had an experience where we counted on someone to show up to get work done, and we can all share experiences when they simply did not show up. Failure to show up for an appointment is not only inconvenient, but it can also cost your customer a lot of money in lost time and productivity.

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. When that happens, call the customer as soon as you know and give them your best estimate of when you can be there. 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 is at risk. Before you work on a computer, always ask if there are backups. If there aren't, offer to make backups for the customer, even if this incurs an extra charge for the customer. If they choose not to make a backup, make sure the customer understands, very clearly, the risk to the data on the system you are about to repair.

NOTE Most PC 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.

Adaptability/Versatility

Adaptability defines how someone adjusts to changes. Versatility, at least within the scope of an IT technician, is bringing a broad set of skills to the PC repair process. Every PC repair is to some degree a guessing game. No one knows all the possible problems that can go wrong with a computer. There is no universal PC repair manual to which you can refer to tell you how to fix computers. Good techs must be able to adapt to any situation, both technically and in the environment. For example, good techs should be able to fix most peripherals, even if they are not experts on that particular device. As you progress through the book, you'll discover that most devices fit into one family or another and that there are certain diagnostic/repair steps that you can at least try to enact a repair.

Adaptability isn't just for technical issues. PCs find themselves broken in the strangest places and ways. An adaptable tech doesn't have a problem if a computer sits at the top of a suspension bridge or behind a desk. An adaptable tech can work around mean dogs, broken water lines, and noisy little kids. (But there are some very important rules to dealing with kids. See later in this chapter.)

A technician has to be versatile. The best example of this is what I call the User Advocate. User Advocates are technicians who take the time to learn the processes of whatever organization they work for and look to create technology solutions for problems and inefficiencies. This also means a tech should be at least competent if not expert at all the computer applications used by the organization. When you combine your IT skills with an understanding of how the business works, you become amazingly versatile, quickly finding yourself with more responsibility and (hopefully) more money.

A big part of versatility is offering different repair options in certain situations. When there is more than one way to fix things, make sure the customer knows all the options, but also give them your recommendation. Tell them why you feel your recommendation is the best course of action, but give them knowledge necessary to make their own decision.

A tech's versatility isn't limited to IT skills. Woe to the tech who doesn't understand basic electrical wiring and building codes. I've had hundreds of repair scenarios where the fix was as simple as knowing how to turn on an electrical breaker or moving a PC away from an electrical motor. No, these aren't IT skills, but a versatile tech knows these problems exist.

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 in a place where your customer can hear. 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. When in doubt, always ask the customer for guidance.

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 PC got into the state it's in takes skill. Communicating clearly and effectively is important. Plus, you need to follow the rules of tech-person decorum, acting with personal integrity and respect for the customer. Finally, use assertive communication to empathize with and educate the user. Great techs spend the time needed to develop these essential skills.

Assertive Communication

In many cases, a PC 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 makes you sound accusatory.

The second part of assertive communication is making sure you state the problem clearly without accusing the user directly: "Not keeping up with defragmenting your hard drive slows it down," or "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

The final key in communicating with users revolves around *respect*. 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.

Generally, IT folks are there to 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.

Don't assume the world stops the moment you walk in the door and that you may immediately interrupt their 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. Take the time to listen. Don't interrupt customers as they describe 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.

Remain positive 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. Take it in stride; smile, and assure him that computer troubleshooting sometimes takes a while.

Avoid letting outside interruptions take your focus away from the user and her computer problem. Things that break your concentration slow down the troubleshooting process immensely. Plus, customers will feel insulted if you start chatting on your cell phone with your significant other about a movie date later that night when you're supposed to be fixing their computers! You're not being paid to socialize, so turn those cell phones and pagers to vibrate. That's why the technogods created voicemail. 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.

If you discover that the user caused the problem, either through ignorance or by accident, don't minimize the importance of the problem, but don't be 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.

Eliciting 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. Once the person has described the situation, you must then ask questions. This process is called *eliciting answers*.

Although each person is different, most users with a malfunctioning computer or peripheral will be afraid and often defensive about the problem. To overcome this initial attitude, you need to ask the right questions *and* listen to the customer's answers. Then ask the proper follow-up questions.

Always avoid accusatory questions, because they won't help you in the least (Figure 2-4). "What did you do?" generally gets a confused or defensive "Nothing"

Figure 2-4
Never accuse!

in reply, which doesn't get you closer to solving the problem. First, ask questions that help clarify the situation. Repeat what you think is the problem after you've listened all the way through the user's story.

Follow up with fact-seeking questions. "When did it last work?" "Has it ever worked in this way?" "Has any software changed recently?" "Any new hardware?" Ask open-ended questions to narrow the scope ("What 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 (Figure 2-5). 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.

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 them. Wherever possible, avoid using jargon, acronyms, or abbreviations specific to computers. They simply confuse the already upset user and can make you sound like you're talking down to them. 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 PC 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!

Figure 2-5
Keeping it friendly

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 PCs 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 them thinking about you, should they need more help in the future. Here are a few items you should consider.

Time Frame

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 them what you'll need to know before you can make the prediction.

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 them as soon as possible. Let them know what's happened, why you're going over, and give them 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, especially when a precious computer is at stake.

Documentation

At the completion of work, document the problem, including the time and day you started work, the solution (again including the time and day the work ended), the hours worked, and a list of all parts replaced. If the customer owns the 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

I call follow-up the Lost Art: a 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 gives that final extra touch that ensures they will come to you again.

Safety and Tools

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 the computer. That starts with knowing how to handle computer components safely and how to use the tools of a tech. Let's begin by identifying and discussing some of the problems you may run into and how to deal with them.

Electrostatic Discharge (ESD)

If you decide to open a PC while reading this chapter, as I encourage you to do, you must take proper steps to avoid the greatest killer of PCs: *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 your PC, so it is essential that you take steps to avoid ESD when working on your PC.

NOTE All PCs are well protected against ESD on the outside. Unless you take a screwdriver and actually open up your PC, you don't need to concern yourself with ESD.

Anti-static 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 PC you touch at the same electrical potential. You can accomplish this by connecting yourself to the PC via a handy little device called an *anti-static wrist 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 PC and place the wrist strap on either wrist. Figure 2-6 shows a typical anti-static wrist strap in use.

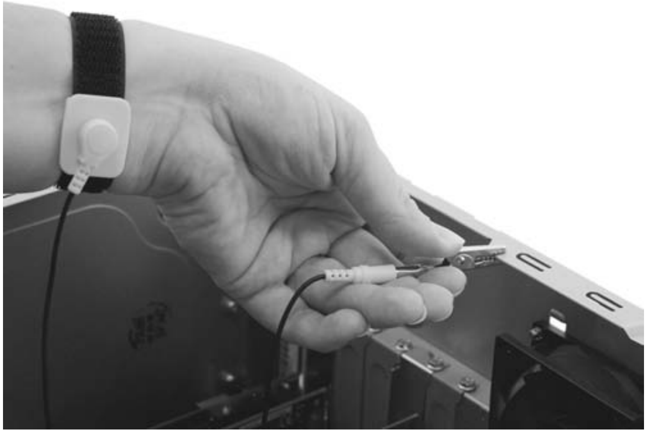


Figure 2-6 Anti-static wrist strap in use

EXAM TIP Static electricity, and therefore the risk of ESD, is much more prevalent in dry, cool environments.

Anti-static wrist straps are standard equipment for anyone working on a PC, but other tools might also come in handy. One of the big issues when working with a PC occurs if you find yourself pulling out parts from the PC and setting them aside. The moment you take a piece out of the PC, it no longer has contact with the systems and may pick up static from other sources. Techs use anti-static mats to eliminate this risk. An *anti-static mat* acts as a point of common potential; it's very common to purchase a combination anti-static wrist strap and mat that all connect to keep you, the PC, and any loose components at the same electrical potential (Figure 2-7).

Anti-static wrist straps and mats use tiny *resistors*—devices that stop or *resist* the flow of electricity—to prevent anti-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 anti-static tools to see how to test those small resistors properly.

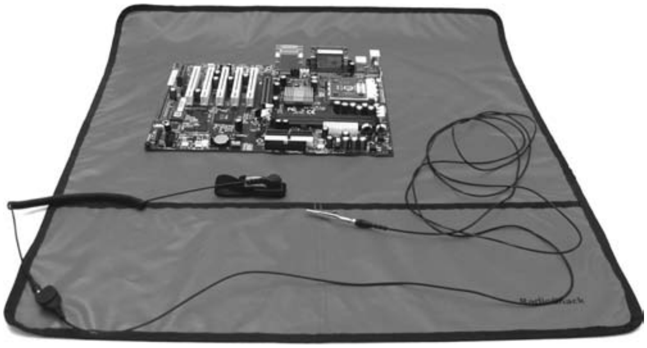


Figure 2-7 Anti-static wrist strap and mat combination

Any electrical component not in a PC needs to be stored in an *anti-static bag*, a specially designed bag that sheds whatever static electricity you have when you touch it, thus preventing any damage to components stored within (Figure 2-8). Almost all PC components come in an anti-static 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 2-8
Anti-static bag

EXAM TIP Always put components *in* an anti-static bag, not *on* the bag.

Although having an anti-static 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 anti-static tools. This shouldn't keep you from working on the PC—if you're careful! Before working on a PC 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 3, "The Visible PC"—to keep yourself at the same electrical potential as the PC. Although this isn't as good as a wrist strap, it's better than nothing at all.

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

EXAM TIP Always unplug a PC when working inside it.

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. Never get a magnet close to:

- Floppy disks
- Hard drives
- Flash drives
- CRT (tube) monitors

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 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 others' frequencies. In Chapter 24, "Working With Wireless," you'll see how to tune a wireless network to prevent RFI.

Protective Packaging

Computer gear manufacturers package their product 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 Figure 2-8) you'll see hard drives packed in, for example, and the black and silver woven bags you'll sometimes see.

A word of caution is in order here. The metal bags provide proper protection only when sealed, so fold the open end over and slap a piece of tape on it when storing a component.

Physical Safety

IT techs live in a dangerous world. We're in constant danger of tripping, hurting our backs, and getting burned by hot components. Let's take a moment to discuss these three physical safety issues and what to do about them.

If you don't keep organized, hardware technology will take over your life. Figure 2-9 shows a corner of Mike's office, a painful example of a 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 (CompTIA calls these folks "building services") to take care of it immediately. The results of ignoring such hazards can be catastrophic (Figure 2-10).

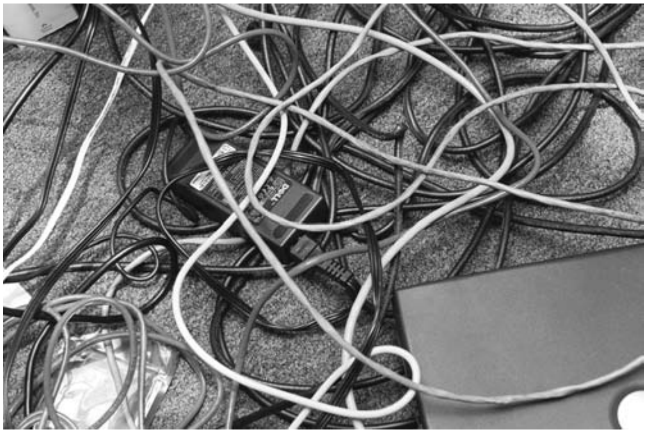


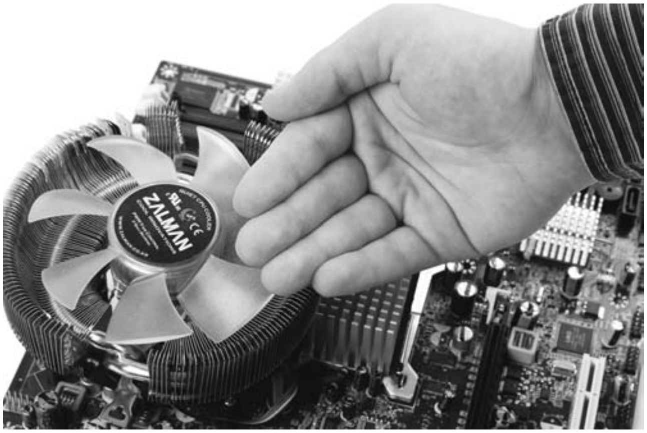
Figure 2-9 Mike's cable kludge

Figure 2-10
What a strange, bad trip it's been.

Another physical safety issue is heavy boxes. Computers, printers, monitors—everything we use—all seem to come to us in heavy boxes. Remember never to lift with your back; lift with your legs, and always use a hand truck if available. You are never paid enough to risk your own health.

The last physical safety issue to discuss is burns. The computing world is filled with hot components. It's hard to burn yourself unless you actually open up a computer, printer, or monitor. First, watch for anything with a cooling fin like the one shown in Figure 2-11. If you see a cooling fin, odds are good that something is hot enough to burn you. Also look for labels/stickers warning about hot components. Last, when in doubt, move your hand over components as if you were checking the heat on a stove.

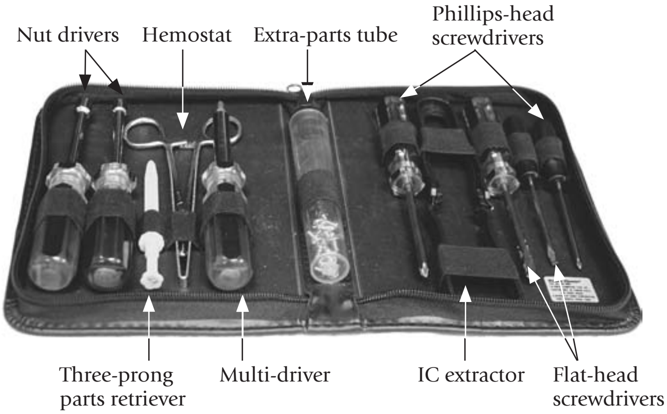
Figure 2-11
Checking for hot cooling fins



Tools of the Trade

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*), and a hemostat to go along with Phillips-head and flat-head screwdrivers (Figure 2-12).

Figure 2-12 Typical technician toolkit



A lot of techs throw in an extension magnet to grab hard-to-reach bits that drop into cases. 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.

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. While manning the help desk, you get a call from Sharon in accounting. She's lost a file that she knows she saved to her hard drive. Which of the following

statements would direct Sharon to open her My Documents folder in the most efficient and professional manner?

A. Sharon, check My Documents.

B. Sharon, a lot of programs save files to a default folder, often to a folder called My Documents. Let's look there first. Click the Start button and move the mouse until the cursor hovers over My Documents. Then press the left mouse button and tell me what you see when My Documents opens.

C. Probably just defaulted to My Docs. Why don't you open Excel or whatever program you used to make the file, and then open a document and point it to My Documents?

D. Look Sharon, I know you're clueless when it comes to computers, but how could somebody lose a file? Just open up My Documents, and look there for the file.

4. What tool should be in every technician's toolkit?

A. Pliers

B. Hammer

C. Straight-slot screwdriver

D. Phillips-head screwdriver

5. 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.

6. When troubleshooting a software problem on Phoebe's computer and listening to her describe the problem, your beeper goes off. It's your boss. Which of the following is the most appropriate action for you to take?

A. Excuse yourself, walk out of the cube, and use a cell phone to call 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.

7. 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.

8. 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 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.

9. 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. Anti-static spray

B. Anti-static bag

C. Anti-static wrist strap

D. Phillips-head screwdriver

10. Which of the following helps prevent electromagnetic interference?

A. Use an anti-static bag.

B. Use an anti-static wrist strap.

C. Keep magnets away from computer components.

D. Keep computers away from monitors.

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 on.
3. **B.** Walking customers through the path to a fix by using simple, nontechnical words is the best way to accomplish tasks over the phone.
4. **D.** Every tech's toolkit should have a Phillips-head screwdriver, at the very least.
5. **D.** Don't get angry or yell at clients.
6. **D.** Focus on the customer and don't use her things.
7. **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.
8. **A.** A simple follow-up builds good will and trust. This is a very important step to take after completing a job.
9. **C.** An anti-static wrist strap keeps you at the same electrical potential as the computer.
10. **C.** Avoid putting magnets near computer gear to help prevent EMI.