The 10 most important things to teach your users

Version 1.0
May 31, 2006

By Becky Roberts

To be effective in their jobs and contribute value to the business, users need at least a minimal grasp of information technology. Exactly what they need to know varies greatly from environment to environment. But in most organizations, they should at least be able to understand and follow certain computing best practices, including how to effectively report problems and how to safeguard their data. Frequently, it becomes the responsibility of the support tech to impart this information. Here are the things I believe are most important for support techs to teach their users. Feel free to challenge these suggestions and add some of your own.

1 Rebooting before calling for help

Although telling users to reboot when they experience a problem may seem like a cop out or delaying tactic, it's an uncomfortable fact that rebooting apparently fixes a multitude of both real and perceived errors. Even if a reboot does not solve the problem, the mere fact that the problem recurs after a reboot can give the canny support tech significant diagnostic information. Rebooting is not a panacea for all computer ailments, and it's even contraindicated in some cases, but appropriately and correctly applied it's a useful and simple tool with which to arm your users.

2 Reporting a computer problem

In addition to knowing the correct procedure for reporting computer problems--e.g., e-mailing the help desk--users need to know what information will help expedite the resolution process. Users can easily be trained to effectively report problems if they're provided with a form that gathers the appropriate information, such as any error messages, open applications, what were they doing when the problem occurred, and whether they can reproduce the problem. Consistently asking users these questions will also serve as training and will help prevent them from either giving too little information or from offering their diagnosis of the problem instead of the symptoms.

3 Keeping passwords safe

There is little point in having a password if it's written down in an unsecured location or shared among co-workers. I have seen passwords written on post-it notes attached to monitors, inscribed in permanent ink on the side of computer cases, written on the backs of hands, pinned to notice boards, and even displayed as the text of the Marquee screensaver. Instructing users not to write down or share passwords has little impact, however, if they don't understand why that's risky or if the password policy is unnecessarily onerous for the environment. On the other hand, an intelligently conceived password policy, suited to the current security needs and well communicated to users, will definitely cut down on the incidence of password carelessness.

4 Constructing secure passwords

While educating users about the importance of securing passwords, take advantage of the opportunity to provide instruction in the art of secure password formation. To a certain extent, password construction is dictated by the constraints implemented through the security system, but in most cases these constraints aren't sufficient to prevent users from creating easily deciphered passwords.

What constitutes a secure password will vary depending on the environment, but typically, names of family members, sequencing numbers, and obvious words and phrases should be avoided. Random numerals and a mix of cases, punctuation, and spaces is generally encouraged. Obviously, a balance between security and convenience must be found. If the requirements for complexity are too stringent, users will simply revert to writing down their passwords. For more information on secure password construction, check out the PowerPoint presentation Raise user awareness about password security and the article "Help users create complex passwords that are easy to remember."

5 Practicing safe computing while traveling

Taking a notebook, PDA, or other device on the road requires increased vigilance to prevent unauthorized access. Users need to know how to protect their data while out of the office and they need the appropriate tools to do it. For example, remote access tokens should not be carried in the same case as the computer; access codes, names, and passwords should not be written down; sensitive data should be encrypted and/or stored on removable data storage devices, also carried separately from the computer; computers should never be left unattended; and consoles should be secured when not in use. See "10 things you should do before letting users take their laptops out the door" and "End user laptop: Lock it down in 10 steps" for more best practices.

As a footnote, this might also be an opportune time to remind notebook users that they will keep us very happy if they remember to remove all solid objects, usually pens, from their keyboards before slamming down their lids.

6 Preventing loss of data

Users need to know that backups don't happen by magic, and that if they delete a file before it has been backed up, it may not be recoverable. In most environments, individual users are at least partially accountable for regularly backing up their data, regardless of whether it resides in discrete files or within an application. Users need to know what's backed up and when and not simply assume that every file they create or modify, regardless of location, will be backed up.

This is particularly true for users with notebooks, removable drives, and other mobile devices. Making users aware of backup routines may also have the usually desirable side effect of reducing the number of non-work related personal files saved to backed up locations. "10 things you can do to protect your data" will give your users a good overview of the basic concepts of data security.

7 Observing usage policies (No, it's not okay to hide pornography in Word docs or install Dr. Seuss Reading Games on "your" computer…

…for your five year old to play over the weekend and then remove it before returning to the office on Monday.) When it comes to personal use of corporate IT resources, most organizations have some sort of policy, more or less stringently enforced, defining what is and what is not acceptable usage. Generally speaking, such policies are put in place to protect the company from lawsuits and to protect the integrity of the IT infrastructure. To be effective, such policies must be appropriate for the environment, be clearly communicated, and be enforceable with well-defined consequences for violators.

Regardless of the strength or content of the policy, we would like our users to know that it is not acceptable to violate it, especially not in sneaky ways that insult our intelligence. In addition to knowing the policy, users need to know that we have measures in place for detecting attempts at violation. As much as we don't wish to play the role of compliance police, we are forced to do so to protect our network and our jobs. This information security policy includes sections on acceptable usage of company computer resources.

8 Exercising care in sending e-mails

How many times have you been asked to recall an e-mail accidentally sent to the wrong person or persons? Over the years I have seen the following messages misdirected: termination notices, pay raise denials, extremely personal medical information about a girlfriend sent to the user's wife, and images of a very questionable nature accidentally sent to the director of human resources. Regardless of an organization's e-mail policy, users need to be aware of this danger and be taught to exercise appropriate caution: Think before pressing Reply To All, double-check addressees before clicking Send, refrain from using the corporate e-mail system for non-business related messages, and in general, regard e-mail messages as postcards instead of letters.

9 Protecting against viruses, phishing, malware, and other nasties

Although it is usually the responsibility of the IT professionals to protect corporate resources, this protection can never be 100 percent foolproof, so we are forced to depend on the vigilance of the user. Users need to be taught to recognize and handle threats and the consequences of not doing so. They need to be provided with specific information on how to identify phishing and how malicious e-mail can appear to be from a legitimate contact. They should be warned not to open e-mails from unknown sources, not to open unidentified attachments, not to enter their corporate e-mail address on Web sites, and not to turn off any protection on their computer. They should be understand the need to stay on top of antivirus updates. Frequent reports of new threats and statistics of how many viruses have been caught within your organization can also help raise their security awareness.

10 Remembering that support techs work most effectively when adequately supplied with chocolate

This requires no further explanation.

Becky Roberts has worked as a database developer for the British aerospace industry, a mainframe programmer for a ceramics manufacturer, an applications developer for an employment agency, and an IT-do-everything person for international management consultants. She's currently playing with the networks in a chemical plant in Texas. Becky is an avid mountain biker and rock climber; she lives in inner-city Houston with too many pets, including four cats, three ferrets, and two teenagers.

Additional resources

- TechRepublic's Downloads RSS Feed XML
- Sign up for TechRepublic's Downloads Weekly Update newsletter
- Sign up for our Desktops NetNote
- Check out all of TechRepublic's free newsletters
- "10 dumb things users do that can mess up their computers" (TechRepublic download)
- "The 10 worst ways to communicate with end users" (TechRepublic download)
- "10 classic clueless-user stories" (TechRepublic download)
- "10 improvement goals for the less-than-perfect end user" (TechRepublic article)

Version history

Version: 1.0
Published: May 31, 2006

Tell us what you think

TechRepublic downloads are designed to help you get your job done as painlessly and effectively as possible. Because we're continually looking for ways to improve the usefulness of these tools, we need your feedback. Please take a minute to drop us a line and tell us how well this download worked for you and offer your suggestions for improvement.

Thanks!

—The TechRepublic Downloads Team