

Top 10 Security Mistakes

REPRINTED FROM: *Computerworld*
JUL 9, 2001 ARTICLE ID: 793

by Alan S. Horowitz

You may not be able to prevent serious break-in attempts, but you can at least avoid leaving your doors open at night.

People regularly lock their houses, demand airbags in their vehicles and install smoke alarms in their homes. But put them in front of a computer, and you'd think the word security was magically erased from their brains. People are more careless with computers than perhaps any other thing of value in their lives. The reason is unclear, but observers agree that end users -- and even some IT departments -- can be pretty dumb when it comes to protecting computers and their contents.

The following are some notable, less-than-bright errors that people and IT professionals commit when it comes to computer security:

1. **The not-so-subtle Post-it Note.** Yes, those sticky yellow things can undo the most elaborate security measures. Too lazy to remember their passwords, users place them where they -- and everyone else -- can see them: stuck to the front of their monitors. Lest you think this is so obvious it's uncommon, Garrett Grainger, vice president of information systems at office supply manufacturer Dixon Ticonderoga Co. in Heathrow, Fla., estimates that of his several hundred end users, 15% to 20% regularly do this.
2. **We know better than you.** You may think that certain security measures are necessary, but not all end users agree, which leads them to do an end-run around you. "People blithely turn things off they think have a good reason to bypass," notes Frank Clark, network operations center manager at Thaumaturgix Inc., an IT consulting firm in New York. "Antivirus software is an example. They think it slows down their machine."
3. **Leaving the machine on, unattended.** Dan Bent, CIO at Benefits Systems Inc. in Indianapolis, says he's amazed at the number of users who leave their machines on, without protection, and walk away. Who needs a password?
4. **Opening e-mail attachments (remember the Love Bug virus?) from mere acquaintances or even strangers.** This one drives IT managers nuts. "Users open all their e-mail attachments before thinking," says Marie Phillips, manager of information security services at Amerisure Mutual Insurance Cos. in Farmington Hills, Mich. "We tell them to be careful about opening notes and attachments from strangers or when they get the same notes from several people, even those they know."
5. **Poor password selection.** If there's a bugaboo among security experts, it's poorly chosen passwords. Ken Hill, vice president of IT at General Dynamics Corp. in Falls Church, Va., recently attended a demonstration with about 20 of his top engineers and some antihacking experts from NASA. Within 30 minutes, the NASA folks broke 60% of the engineers' passwords. Paul Raines, global head of information risk management at London-based Barclays Capital, recommends that users take a common phrase and use its initials for a password. For example: "I pledge allegiance to the flag" becomes "ipa2tf." "That's a difficult password to break because it's a combination of letters and numbers," says Raines.
6. **Loose lips sink ships.** Clark says people often talk in public places about things they shouldn't. "They will say at a bar, 'I changed my password and added the number 2,' and someone sitting two stools down hears this. Some things you just shouldn't talk about outside the office environment," says Clark.

7. **Laptops have legs.** Everyone knows how common it is for laptops to be stolen in public places, but Jay Ehrenreich, senior manager at PricewaterhouseCoopers in New York, says it's surprisingly common for a person to leave his laptop in his office, unsecured and unattended, and in full view of passersby. "These things walk," he warns. Users should place their laptop securely out of sight, such as in a locked desk drawer.
8. **Poorly enforced security policies.** The best-designed security plans are useless if IT fails to rigorously enforce them. "If these things aren't enforced by the system, then the policy isn't useful," notes Chris Smith, vice president of computer information systems at EasCorp, a Woburn, Mass.-based provider of wholesale financial services to the credit union industry.
9. **Failing to consider the staff.** "Your greatest [security] threat is from in-house," says Hill. Disgruntled employees and others can cause enormous problems if they're not properly monitored. IT departments should do a good job monitoring incidents and have the forensics capabilities to be able to follow problems to their sources.
10. **Being slow to update security information.** "One thing we see all the time is that service packs are not kept up-to-date," says Ehrenreich. This creates a window of opportunity for hackers.