10 Essential Things Companies Should Teach Employees About Security

By: Don Reisinger
2009-10-29

10 Essential Things Companies Should Teach Employees About Security

News Analysis: As many security systems as an organization might have, the last line of defense rests with the employees. That's precisely why companies need to do a good job of educating employees about security. Employees have to be directly engaged in the IT security process.

When it comes to enterprise security, ensuring that sensitive data doesn't find its way out and beyond the control of the office is a major concern for most companies. That's why they enlist the help of security software, hardware systems and anything else that can possibly keep data secure. It's a smart plan. And for the most part, it does help companies keep much of their data secure.

But there is another major security hole at many companies: the employees. Too often, it's the average employee who allows malicious hackers to make their way into corporate files, steal sensitive data and wreak havoc on productivity.

That's why. They need to remind them about the dangers of letting malicious hackers into the network. And they need to do it now.

Here are 10 things every company should teach its employees about security.

1. E-mail is a killer

One of the easiest ways malicious hackers can make their way into a corporate network is through e-mail attachments. Hackers spoof the sender's address, making recipients feel comfortable; when the employee opens the attachment and allows an executable file to run on the system, trouble erupts. Companies need to remind employees to only open attachments from trusted—even impeccable—sources that are about relevant and current business. There's no telling what might be hiding in attachments from random e-mails that make it through the corporate spam filters.

2. Social networks can't be absolutely trusted

Too often, employees believe that a social network like Facebook or Twitter can be trusted. Any link on the site can be safely opened, they reason. They're wrong. Facebook has been hit by security issues. Twitter users have gotten in trouble by clicking links in tweets that brought them to malicious sites. Social networks can be dangerous.

Employees need to realize that.

3. Keep definitions up-to-date

It might be annoying when a security program wants to run virus definition updates once a day or sometimes several times a day. But it's a necessity. Employees that ignore those updates are putting themselves, their computers and their company at risk. Whenever a definition message pops up, employees should be taught to download those definitions immediately. There's no telling what's out there just waiting for that computer that hasn't been updated.

4. Deploy security patches to everyone

Although many companies patch Windows centrally, there are still some organizations that don't automatically update users' computers. When that happens, employees need to be aware that updating their Windows installations is just as important as keeping their virus definitions updated. An unpatched Windows is an unsafe Windows.

5. Remember Web security

Employees should be told that surfing to unknown sites is a significant breach in security. Too often, employees travel to sites they may never have heard of, only to find that malicious files have been downloaded onto their computers. Companies should make it clear to employees that they should only travel to trusted sources that are required for business activities while in the office. Accessing any other site could wreak havoc on the corporate network.

6. Password security

Although simple passwords might be easier to remember, for employees to use "1-2-3-4" as a password to gain access to a corporate computer is unacceptable. Employees need to be taught how to create a secure password. It should be alphanumeric and include at least one symbol and uppercase letters. The easier the password is to break, the sooner someone will be able to hack into the corporate network. Password security on all computers is extremely important.

7. Keep locks on computers

Since so many employees are going mobile these days, ensuring that no one steals a laptop is becoming an even greater concern. Companies should provide employees with laptop locks. They should also teach those employees how to use those locks. It's important to remind them that locking a laptop to an immovable object is step one.

8. Use encryption software

Thanks to Windows 7, users will now be able to encrypt files on an external hard drive or

USB key with BitLocker To Go. It's a great solution. But it only works if employees know how to use it. Companies should do their best to explain the importance of encryption to employees. They then need to teach employees how to use encryption tools like BitLocker to ensure that the contents won't be easily accessed when portable data is misplaced.

9. Educate workers about corporate security policies

It's important for employees to know not only that there is a corporate security policy in place, but that there are rules that they need to follow. They should also be aware that if they break those rules, there will be consequences. When they know that there are ramifications, they may be less inclined to engage in dangerous behavior. The security policy is the first line of defense against malware. It can't be taken lightly.

10. The threats are real

It might sound simplistic, but employees can't be expected to engage in fully secure behavior until they understand the ramifications of security issues. They need to know that if a hacker breaks into a corporate network, it could ruin the entire organization. It could also put their jobs in jeopardy. Network security is a dangerous game. And until employees are taught that, they might not take security policies too seriously.