

TechTalk: Practical IT Security Tips

Protection now easier, cheaper

By **MJ Shoer**

June 12, 2009 6:00 AM

When most people think about security, they simply think of their password, which is hopefully secure. By secure, I don't mean using your birthday or a four-digit number as your password. By secure, I mean a complex passphrase or password with at least one lower-case letter, one upper-case letter, one number and preferably one symbol. While a password of at least eight characters that includes these elements will probably be secure, a passphrase, which is a combination of words strung together, will be even more secure. However, a secure password or passphrase is only the tip of the iceberg.

Proper information technology security also involves how you store and use information. For example, if you are a regular user of e-mail, have you ever e-mailed a password? Have you ever e-mailed your Social Security number or a credit card number? If the answer to any of these questions is yes, I strongly recommend you get yourself some training on IT security. You should never e-mail a password, Social Security number or credit card number. Doing so is akin to opening your office windows and shouting it out loud to anyone who can hear you. While at that particular moment in time no one may be listening, the very real risk is that someone one day will be — and will instantly have access to confidential information that will allow them to potential steal your identity or, possibly worse, hack in to your company's IT network. Believe it or not, this is how a lot of data breaches begin — with someone e-mailing a confidential piece of information that should have never been communicated that way. Always remember e-mail is not a secure communication medium.

Technologies exist to make e-mail communication secure. E-mail encryption scrambles data sent in an e-mail message so it is secure and accessible only to the person or people you authorized to receive the message. While historically, these technologies have been expensive and difficult to use, these barriers are lowering considerably. They are both affordable and considerably more convenient to implement, even when you need to communicate with someone who is not very technically savvy.

For example, imagine a doctor's assistant who wants to e-mail a patient with details about a medical procedure or an accountant who wants to e-mail a client about a tax return. To do so via standard, insecure e-mail would be a violation of privacy laws that govern both of these professions. However, if they were to implement and use encrypted e-mail, they would be able to safely carry on these electronic conversations while guaranteeing security and compliance for their businesses and customers.

Do you use a laptop that you also save confidential data on? If so, unless you are encrypting the hard drive on which that data is saved, you are potentially putting that data at risk. A high number of data security breaches involve the loss or theft of laptops with confidential data on them. Had users of those lost or stolen laptops used drive encryption, data on those drives would have been useless to anyone other than the original user of the system. This is because encryption technologies use a series of "keys" that encrypt the data and make it accessible only to the person who created this key.

The same holds true for universal serial bus (USB) storage devices. These small, highly portable devices are becoming very popular. Many people carry them on their key chains. Like a hard drive, if these keys are not encrypted, data on them is accessible to anyone who can gain physical access to the device, so it's important to properly secure them. Again, technology exists, is affordable and is not difficult to implement or maintain. If you deal with confidential data, please ensure you do so securely. To not do so is simply not worth the risk.

MJ Shoer is president and virtual chief technology officer of Jenaly Technology Group, a Portsmouth-based outsourced IT services provider. E-mail him at mshoer@jenaly.com.