

## **10 Technology Gotcha's Every Business Manager Everybody Should Know**

In today's connected electronic world, we rely on technology to get the job done. But in this space, what you don't know *can* hurt you. With one click a disgruntled employee can send your confidential business intelligence, bank account number and password, or intellectual property to millions of Internet users. In one more click a large portion of your business data could be deleted. The list goes on. Read on for the top 10 Technology Gotcha's; the misconceptions and flaws that are the most likely to get small and large businesses alike in trouble, and some simple ways to avoid them and navigate around the wreckage.

### **1. Physical access is total access!**

Without special precautions, anyone who has physical access to a system can access any data stored on that computer. Most computer accounts can be cracked in under 30 seconds when you have physical access to the system, or the accounts can be bypassed altogether. Use hard disk passwords to lock traveling laptop systems. Keep servers and computers with sensitive data physically secure.

### **2. People Make Security, Computers Don't!**

The biggest security threat to your business is people, whether it be simple mistakes or malicious intent. Create a formal information security policy and make sure your staff signs off on it. Do not allow staff to share accounts on any system or software package. Delete general accounts or guest accounts, and always change default passwords.

Only management or IT staff should have access to the Administrator or Root account. These should not be shared with general staff or used for daily tasks, and passwords should be changed frequently to monitor access.

### **3. Email is public!**

Typical email access, via the Internet or an email client, transmits not only

your email messages to the public, **but your password too**. Use secure authentication (SSL) to prevent your email password from being broadcast to the public.

Email messages are *never* private (**even when using SSL**), unless you specifically encrypt the content. Omziff is a free utility to encrypt documents-- use blowfish encryption: it takes 400 years to crack with today's best desktop computer vs. your typical document 'password' protection that cracks in less than 30 seconds. Always give out the encryption password separately and in person.

If you receive confidential information or requests for confidential information via email, please remind the sender that email messages are broadcast to the public across the Internet, and anyone on the Internet can easily read them.

If someone does transmit your confidential information insecurely you should request that the sender pay for identify theft protection or credit monitoring for everyone involved for one year. If it is a vendor, make sure that management knows what has occurred; many states now require businesses or government entities to notify all affected customers when they have experienced a breach of security.

### **4. FTP is not secure!**

If you do need to share confidential information on the Internet, use a secure protocol to do it. File Transfer Protocol (FTP) is a very common way to share files on the Internet. But, it is not secure, *even if* it requires an account and password, the password is transmitted to the public and can easily be compromised. The alternatives are Secure File Transfer Protocol (SFTP) or a secured website (HTTPS).

### **5. Windows@ is wide open!**

All platforms have security vulnerabilities, but Windows@ is generally the most plagued with security issues, probably because it

has the lion's share of users. The three types of security threats to Windows@ computers are malware, viruses, and hackers. Invest in programs or appliances that stop all three. Most security programs are good at stopping just one of these three categories of threats. Once infected these threats typically monitor your system for confidential information and transmit it to the Internet, they may not damage or otherwise disturb your system.

### **6. VPN's are your best friend!**

Virtual Private Networks (VPNs) allow mobile staff to securely access your business network from the Internet. Any messages or files accessed through a VPN are as secure as the network to which the VPN is connected to.

### **7. Passwords are Key!**

Using secure websites (HTTPS) is like talking in a telephone booth vs. shouting in a room full of people: no one else on the net can hear your conversation. But it still does *not* guarantee that you are who you say you are -- your account and password are the only way that most websites can tell who you are. (Banks and other financial sites are inventing more ingenious and annoying ways to verify your identity as we speak.) Anyone can access a secure website and try to crack your account.

Create passwords that are harder to crack: at least 8 characters, with at least one each of numbers, upper case letters, lowercase letters, and symbols.

Use a password trick to create unique passwords for every account you have. Sound impossible to remember? A trick is a process for creating a password. If you remember the trick, you won't need to remember every password you have, and you'll have a unique password for each of your accounts.

For example, a password could be created using an exclamation point, followed by the first and last two letters of the account name, plus the

number of vowels in the account name, plus the user's initials. Using this trick you can generate a unique password for any account you own: 'linkedin' would be: "!liin3seh", and 'Google' would be: "!gole3seh". Have a backup trick (a mild modification to your existing trick) ready in case one of your accounts requires a password change.

Never share passwords with anyone else. If an exception occurs, change your password, then give it to someone you trust, and then change it back after they are finished.

### **8. Historical backups are critical!**

The *only* way to recover from a user mistake is from backups. Historic backups are key. If your backups are simply a copy of your data which is overwritten each time-- then when a mistake is made, and you catch it tomorrow after it has been backed up, your backups are worthless.

Drive mirroring and redundant hardware keeps systems available in case of a hardware failure, but is quite useless against a 'user mistake' that is quickly synchronized across the systems.

Make sure your staff knows where and how they should be storing their data so it is protected by backups. Mobile users should keep their data on the network (via VPN) so it is protected, or have additional backups in place.

### **9. Faxes and Voicemails are public!**

Long gone are the days when faxes and voicemails were secure. Now they are bundled into attachments and sent flying across the Internet to a cell phone or an email inbox. *It can be done securely*, but it's rare these days; always ask when dealing with confidential information.

### **10. You are who you trust!**

When you trust your data to an outside system or vendor, you are responsible to your staff and customers if they make a mistake. Remember that you get what you pay for.

Hosted 'Software As A Service' (SAAS) systems can be very useful and affordable for small businesses, but be careful! These vendors are never responsible if your data is stolen, lost, or damaged-- but you are. Make sure you have data backups and security if needed. Hosted vendors with many customers are "big fish" targets for serious hackers, as all of the data is conveniently accumulated in one place, whereas targeting an individual business might not be worth the hassle.

### **Now you Know...**

why identity theft is so common! If your email password is the same as your stock exchange or bank account password, go change both of them-- right now!

There are simple and low cost solutions that address all of these issues for SMBs, many are simply a point of awareness and training. Now you are gifted (like it or not) with awareness and education to help keep yourself and your business securely afloat in our connected world.

Sheila Hatfield

*Sheila has 14 years experience in the information technology field, and is a founder of Psimetrix Inc. an IT firm serving the greater Denver metro area. She can be reached at 303-469-9763 or sheila@psimetrix.com*