



January Newsletter: Safer passwords and data theft

As customary, we're starting off the year with a few tech-minded office resolutions for you. And since security is always on our minds (especially this holiday season, with its airport madness), we'd like to suggest the following:

1. Resolved, that we'll secure our office passwords and institute a smart password policy
2. Resolved, that we'll protect office data from employee theft

We'll cover some tips and "best practices" to help get your office up to speed on both accounts. This newsletter also features Lisa Perry Style in our Client Spotlight.

Good luck!

Your friends at Cartwheel

Client Spotlight: Lisa Perry Style

Lisa Perry Style is a maker of signature fashion collections for women and girls. They recently opened a new concept store and design studio on Madison Avenue, which – in addition to its mod-inspired couture pieces – will also feature home furnishings and accessories lines, as well as vintage items from the 1960s and 1970s. You can learn more about designer Lisa Perry and Lisa Perry Style at <http://www.lisaperrystyle.com>.

Why do we love Lisa Perry Style? For one, their new store takes over a former bank space, and Lisa utilizes its architectural elements with a whimsical spin. The design staff and office are enclosed in a glass box taking center stage, giving onlookers a view of the upcoming season's collections, inspiration and design boards. Inspired by her passion for 1960's couture fashion and art, Lisa's collection combines geometric shapes with bold colors to create a simple, chic aesthetic.

Secure passwords

With more and more sensitive information kept on the Internet (which we think is a good thing), a solid password policy is the most important defense against unwanted disclosure of your company's data. Even if you keep all your data in-house, a good password policy will prevent lost laptops, angry employees, and even virus attacks from exposing your sensitive information. Most small businesses, however, have no password policy at all. Small business owners, a number of our clients among them, trust their employees and have an "it couldn't happen to me" attitude. Actually it could, and does.



Below, you'll find a simple technique for password security we use and recommend to our small business customers.

Step 1: Create a strong password policy throughout the company. Here are the guidelines:

- a. Passwords must be 8 characters or more (otherwise some websites will reject them, and you'll just need more passwords)
- b. Passwords can't contain a whole word, name, birthday, phone number, home address, or any other information that can be guessed or obtained.
- c. Passwords must contain at least 5 letters, at least 2 numbers, and at least 1 special character (again, this is so that some websites don't reject them)

Strong Passwords	Weak Passwords
j@hn*\$is	hello123
h!2kroo\$	johnsmith99

Step 2: Train everyone in your company to create strong passwords, and make sure they change all their personal passwords (email, computer login, Quickbooks, etc.) to strong passwords. Depending on your company's infrastructure, you may be able to enforce some of these through your server.

Step 3: Create two strong passwords. Call one your "shared" password, and the other your "secure" password. You'll share the regular password with employees for applications and websites that don't house sensitive information. You'll keep the secure password to yourself for applications and websites that have your most sensitive information (banking, salaries, Administrative password, etc.).

Step 4: For each username / password combination you have, create an address book entry (e.g. in Outlook). You can do this elsewhere too, but something that can synchronize with a PDA (iPhone, BlackBerry, etc.) is ideal.

Go to all the applications and websites you use, and change your password to one of your new passwords. Then, instead of writing the actual password in the Contact Notes field (where snooping eyes might find it), simply write the username and then "shared" or "secure" for which password you used. So the Contact Note for Chase.com might be "joe@yahoo.com / secure."

That's it. You're now secure! And if you're having a senior moment when trying to log in somewhere, just go to your contacts list to remind yourself which password you used for that application or site.



Here are some last reminders for passwords:

Do:

Always use strong passwords

Use an entry code for your PDA

Use a password on your computer and a hard drive password on any traveling laptop

Shred your used hard drives

Don't:

Write passwords down on paper

Keep your passwords in a file on your computer

Throw hard drives in the trash (without shredding them)

Share your secure passwords, even with those you trust (they may write them down)

If you need a security review, or want help enforcing a strong password policy, we'd be happy to help. We can also shred hard drives for you when you're ready to dispose of them securely. Call us at 212 206 9619 or send us an email at hello@cartwheelit.com, and we'll respond right away.

Protect your data from theft

If asked to list their company's assets, most small business owners would rank their data (whether it's a client list or other valuable information) among the most valuable. Unfortunately, it's also the most likely to be stolen. A recent study by an Arizona research group and Symantec showed that over 50% of ex-employees admit to stealing data from their employer. That's a lot more than those stealing equipment, or even money.

As a New Year's resolution, we suggest you take the following steps to limit your exposure, and make sure you're not a victim of data theft.

Encrypt your Backups: Most offices back up their data, whether to an online backup site or to a physical device at your office (in fact, we prefer doing both). Make sure this backup system encrypts your data. Encryption will ensure that no one can access that backup data without a password – so in the case that the physical data does get stolen, at least the thief can't get at anything more than a dead hard drive.

Password Policy: Read our article above about password policies. Having a good password policy will allow you to change vulnerable passwords easily, immediately before you let go of an employee. No matter how trustworthy the individual was while under your employment, it's not safe to leave former employees with free access to your data.

PDAs: It is important to ensure that devices like BlackBerry phones, iPods, or other smartphones aren't being used to cart data off at the end of the day. If these devices are office property (such as company-supplied employee BlackBerries), some services will allow you to remotely wipe the data from them if needed.



Shred paper and lock your cabinets: Believe it or not, about 60% of data thefts are on printed paper. Buy a good shredder and shred data you don't need. If you don't already have one, get a lockable cabinet for your sensitive papers, and keep it locked.

Even with these precautions, employees can simply email files to themselves or copy data onto a flash drive. There is software that allows you to track these types of behavior, but that only helps after the fact.

In some cases, a clear corporate policy and non-compete agreements with all your employees are a strong deterrent against data theft: if an employee knows that it's against company rules to set up an auto-forward or send business emails from his or her personal account, that type of infraction is much less likely to occur. If you don't have these in place, talk to your lawyer about setting them up. You'll be happy you did.

As always, if you have any questions or would like help setting up a secure password system or making sure your data stays safe, don't hesitate to call us at 212 206 9619. We'd be happy to help you keep those New Year's resolutions... any time of the year.