SECURITY AWARENESS NEWSLETTER

PAPER FILES HAVE TO BE PROTECTED TOO

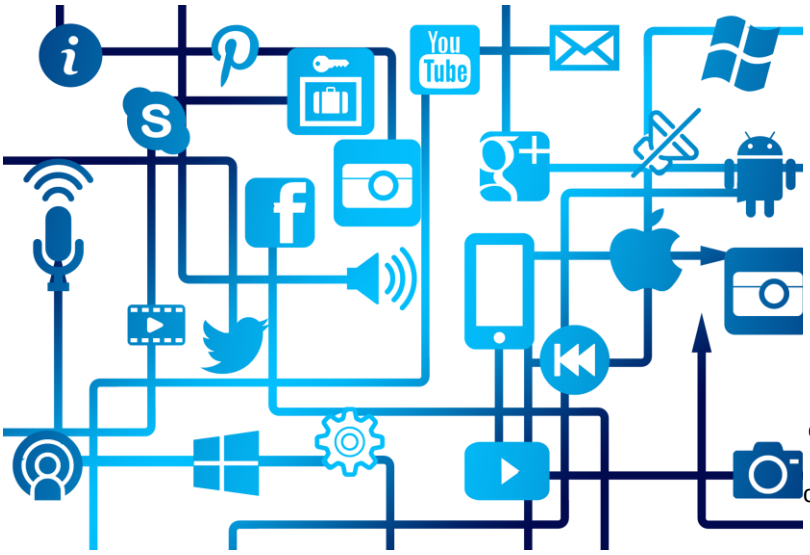
You've probably heard that To err is human, but to foul things up completely you need a computer. We know it's important to protect the big databases that we store, but we can't ignore paper records. The amount of information held on paper may be much smaller, but many of the most serious leaks happen through very human methods — reports stolen from desktops or read over someone's shoulder. Keep sensitive paper files locked away when they are not being used and don't read them in public places.

DO NOT OPEN UNKNOWN OR UNEXPECTED E-MAIL ATTACHMENTS

This morning I got an e-mail from my boss with an attachment. My boss is a man of few words on e-mail. If he wants to explain or discuss something with me, he picks up the phone. When he wants me to read or edit something we have talked about, he sends it to me. Even though the subject line was a date, the e-mail had no text, AND my boss hadn't told me he was sending me an attachment, I opened it because it was from my boss at an e-mail address I recognized. Bad move. Imagine my surprise when my Norton anti-virus screen popped up with a message that the attachment contained a virus and had been deleted. Hackers had spoofed his address and I had fallen for it.

CYBER ZONES
Cyber Security Services

SECURITY AWARENESS NEWSLETTER



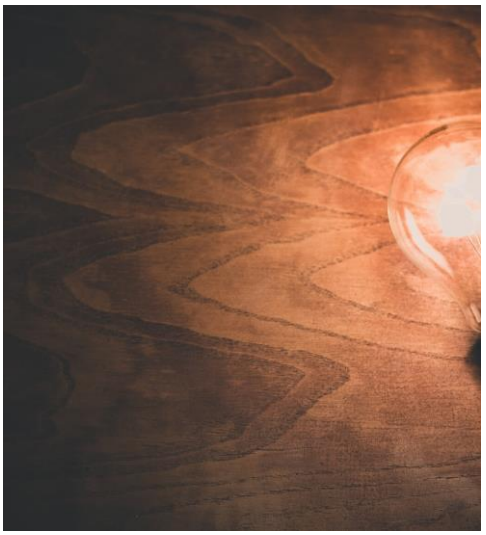
If you access the Internet from a shared computer, make sure you don't leave anything behind

Being able to access the Internet from different locations — the library, a computer lab at school, an Internet cafe — is a great convenience, but it can also pose a security risk to personal information. If you do access the Internet from a shared computer, here are a few things you need to remember.

1. Don't check the "remember my password" box.
2. When you're done, make sure you log off completely by clicking the "log off" button before you walk away.
3. If possible, clear the browser cache and history.
4. Never leave the computer unattended while you're logged in.
5. Trash all documents you used, and empty the recycle bin.

Use variations on a strong "core" password

It's tough to remember a series of strong passwords and use a different one for each online system or site you access. The temptation is to use the same password for several or all systems and sites. That's a bad idea -- if a Bad Guy gets a hold of your password, he'll have the key that fits all of your doors. Instead, create a strong "core" password and then unique variations on it for each online system or site system you use. Here's a strong password: 5P0ky!3Z. It contains 8 characters, a mixture of uppercase and lowercase letters, at least one number and one non-alphanumeric character or symbol, and no personally identifiable information. By adding a character or two at the beginning or the end, you can have many variations to use for each system or site -- effectively creating a new strong password for each one. Remember to change your "core" password and its variations on a regular basis.



Passwords: Be creative

If you can't remember hard passwords no matter how hard you try, put your password in parenthesis. baseball38 is a weak password. (baseball38) is much better.

When you change your password, you should always change at least half of it and when you do, change the parentheses as well. Change the parentheses to asterisks, exclamation points or dollar signs. *sallyandbob39* is better than sallyandbob39, and !jimandbetty93! is better than jimandbetty93.