SECURITY AWARENESS NEWSLETTER

DON'T USE E-MAIL TO SEND PRIVATE MESSAGES

In a hospital romance right out of prime time television, one young woman involved in a three-way love triangle used her personal hotmail account to send romantic messages. She got a response she definitely did not expect: the party she had been cheating on cracked into her hotmail account, printed out some very personal messages and posted them on the message board at the small town supermarket for all to see. Moral of the story: protect your passwords. And PS. As long as you're planning on getting fired, you're better off spending time working on your resume than sending romantic e-mails that you don't want publicized.

EFFECTIVELY DELETE FILES

When you delete a file, depending on your operating system and your settings, the file may be transferred to your trash or recycle bin. This "holding area" essentially protects you from yourself—if you accidentally delete a file, you can easily restore it. An unauthorized person will also be able to retrieve it. Does your recycle bin include credit card information, passwords, medical, or other personal data? Is there sensitive corporate information? Empty the trash or recycle bin on a regular basis to ensure that deleted information stays deleted.

Change the combination on opened laptop locks

When people have cables with combination locks for securing their laptops at their workstation, they always remember to turn the tumblers when they secure the laptop. But what
happens when they unsecure the laptop? Many people won't turn the tumblers on
the opened lock because it is much easier to lock the laptop later if the
combination is already set. About half a dozen laptops in our office
disappeared one day. The laptops were stolen by someone who came by when the
laptops were not there and noted the combination. They came back later when the
laptops were there and used the combination they had noted earlier.

Make your password complex.

Always read the
A good password should contain a mix of all the four
types of characters: uppercase and lowercase letters, numbers, and symbols. Any
character on your Windows or Mac keyboard is legal in a password you make for
your own computer. Remember to include at least 8 characters and avoid common words and proper names. Some characters may be illegal for certain networked systems; when in doubt, try it out. Another way to make your password complex is to base it on a word in a foreign language with a least 8 letters, avoiding common words and proper names. Just add a number, a symbol, and a capital letter or two as you go.

Always log off your own computer. Do not let anyone else offer to do it for you

If One of our branch supervisors was offering to log her staff off for them, so they didn't have to wait, and could get on with their evenings away from work. She wouldn't really log them off, though, but would just turn off their computer monitors. Once the staff had left for the evening, she would go back to the computers to see who was still signed in to the banking software. If she found someone still signed in, the supervisor would then defraud the bank, using her staff's IDs to cover her tracks.