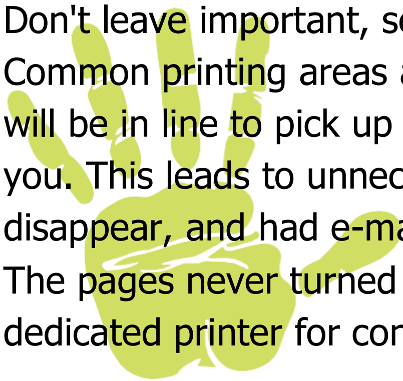
SECURITY AWARENESS NEWSLETTER

DON'T CLICK ON LINKS IN POP-UPS OR BANNER ADVERTISEMENTS

In July 2007, when iPhones were scarce and strongly in demand, Botnet herders put software on already infected computers that redirected users browsing for iPhones to phony websites. The malware caused pop-ups and banner advertisements on infected computers; clicking on the provided links took users to the phony sites. People who attempted to buy iPhones from the sites were actually providing the Bad Guys with their personal and financial information. You can expect to see something similar for any fad that comes along. When your heart is tempted by the latest hot fad, don't throw caution to the wind.

IF YOU PRINT IT, GO GET IT RIGHT AWAY!



Don't leave important, sensitive, or confidential material lying around the office. Common printing areas are frequented by people coming and going. Often you will be in line to pick up your documents and others may handle them before you. This leads to unnecessary information disclosures. One boss had a print job disappear, and had e-mailed the whole floor about it.

The pages never turned up. Always use the closest print station, or a dedicated printer for confidential information, and go get it right away!.

Just because your company's spam filter, virus filter and other defenses let an email through, doesn't mean it's harmless

Last year, one organization narrowly avoided a virus infestation. Alerts led them to the email in-boxes of the virus authors. To sneak in a virus, hackers used encrypted zip files, which went past filters because they couldn't be scanned. The organization caught it with the very last line of defense — desktop antivirus software, which triggered after the users had plugged in the password to see the zip file contents! Had the bad guys written something new, instead of using off-the-shelf script kiddie code that was in standard pattern files, there could have been a major outbreak. Long story short: End-user awareness about email and attachments is every bit as important as antivirus filters and firewalls. EVERY USER is an important part of hacker defense!

Don't buy anything from a spammer

If an unexpected email brings you news that seems too good to be true, it is probably a spam and a scam. If you didn't request information about the product or service, it is probably a spam and a scam. If it promises to enhance parts of your body, it won't. If it promises you an easy mortgage, you can do better by visiting your bank. If it promises that you can make a fortune on a penny stock, you can't. If you are unsure, ask five friends. Chances are four of them also received the spam and you can know to steer clear.

> ***Don't give away your data when you give away your handheld device***
>
> *Be careful before you resell or give away your handheld devices like Palms. The new owner can uncover data. At a minimum, figure out how to reset it to the factory standard. Refer to your manual or call the manufacturer.*