Mundane Science
Bill Downs

Cyber Bad Guys Abound

A computer virus is a computer program. At it's simplest and most benign, it might display a message on your monitor. At it's most destructive, it can erase your hard drive or propagate to other computers, slowing a business network or the Internet itself.

What are the targets for cyberterrorists, cybervandals, and cyberthieves?

Anyone who has a computer that can link to the Internet and potentially anyone who has an electronic appliance with an embedded microprocessor.

Ever watch 'Dark Angel' on Fox? The main character is a product of genetic engineering that lives in a United States reduced to Third World status by a terrorist triggered EMP (electromagnetic pulse). The EMP destroyed all the computers and electronic equipment that was not shielded. Instantly, bank accounts disappeared. Identity files were erased. Cars, trucks, planes wouldn't operate. Industrial plants wouldn't run. No grocery deliveries. No federal, state, or local government. Admittedly, it is a 'doomsday scenario', but it does make you think.

Cybervandals are thrill seekers. They create the newest, most virulent computer virus and release it to create havoc. Why? To show that they can. Hackers will try to crack the uncrackable site to show that they are the best. Thumbing their collective noses at authority. When asked about his motivation by a Congressional Committee, a hacker replied, "My motivation was the quest for knowledge, the intellectual challenge, the thrill, and in order to escape from reality."

Cyberthieves are after information: passwords, account numbers, social security number, birthday, address, phone number, customer data, design data, etc. Any information that can facilitate their current scheme. It might be as small as charging something to your account. They might need to steal your identity. They might be laundering money thru your account. Almost any crime you can think of can be facilitated with a computer and from halfway around the world too

What are the possible targets of the cyberterrorist? Electric power distribution, banking and finance, emergency services, transportation systems, communications networks, and more. All provide essential services. All depend on the free flow of information. All are far-flung, accessible to the public, and hard to defend.

With the coming and going of the latest computer virus, Goner, I thought it would be a good idea to compile a list of ways and ideas for keeping the bad guys away from hearth and home.

- **Do not open** any files attached to an e-mail from an unknown, suspicious or untrustworthy source.
- **Do not open** any files attached to an e-mail unless you know what it is, even if it appears to come from a dear friend or someone you know. Confirm that they really sent it.
- **Do not open** any files attached to an e-mail if the subject line is questionable or unexpected. If you need to, save the file to a floppy and run a virus scan on it before opening the file.
- **Delete** chain e-mails and junk e-mail. It is spam.
- **Do not download** any files from strangers.
- **Exercise caution** when downloading files from the Internet. Make sure your anti-virus program is running and checking the incoming file. Make sure the source is reputable and legitimate. If you're not sure, don't download the file or download the file to a floppy.
- **Update your anti-virus software regularly.** That includes the virus signature files and the scanning engine as well.
- **Back up your files on a regular basis.** If a virus destroys files, you can replace them and only have to reconstruct the data since the last backup. Keep the backups totally separate from the computer they're for. If possible, keep sensitive data off-line altogether and run applications with data on a floppy or zip disc.
- **Always err on the side of caution,** when in doubt and do not open, download, or execute any files or e-mail attachments.

- **Subscribe** to a virus alert service like McAfee or Symantec. You can report a suspected virus to them too.
- **When in doubt,** ask for help.
- **The easier a password** is for you to remember, the easier it is for a hacker to discover**.** Passwords should be combinations of upper and lower case letters, numbers, and characters. The more sensitive the data, the longer the password. Use different passwords for different systems. Change passwords frequently.
- **Check your security setting** for Microsoft Internet Explorer, go to <tools>, <internet options>, <security>, <internet>, <medium security level> at a minimum.
- **Install a firewall,** especially if you have a cable modem or DSL connection.
- **Do not divulge** personal information or system information to anyone unless you are certain who they are and why they want the information.
- **Shred important documents** so they can't be reassembled**.**
- **Physically destroy CD's and diskettes,** because deleted or erased data can be recovered.

Bill Husted, Atlanta Journal-Constitution, 12/16/01, pg. E1
http://www.pcworld.com
Susan Gast, Atlanta Journal-Constitution, 11/4/01, pg. P7
Mike Toner, Atlanta Journal-Constitution, 11/4/01, pg. A4