

# emerging Security threats and Steps for Staying Ahead of the Game

Personal computers continue to be everywhere. Technology vendors are working hard to develop the latest operating system, application, or system that would make the lives of PC users easier, through sexy user interfaces and other bells and whistles that are intended to give the PC user a “pleasurable” computing experience. In the quest for “first to market,” vendors are rushed to put out new software and application without adequate testing; worse, vendors aren’t building security measures into these technologies.

I don’t see this paradigm changing anytime soon – users will continue to demand cool applications, awesome games, office productivity software, as so on. Vendors and manufacturers will continue to quench users thirst to produce these software and leave the security of these technologies up to the “security products” (firewall, anti-virus, etc.) to address and deal with.

Moreover, the underground, hacking, and security research communities are constantly making advancement to identify and discover vulnerabilities and exploits. Zero-day exploits – vulnerabilities that are discovered (and exploited) before vendors provide fixes/patches – will continue to thrive. Remember iPhone? Within two weeks of part-time work, researchers discovered security vulnerabilities with the product.

In this article, we will review some of the emerging security threats that PC users face constantly and steps for making your PC more resilient to emerging attacks.

## EMERGING SECURITY THREATS TO PC USERS

Computer users are plagued with many security challenges that must be dealt with proactively. Computer can never be adequately secured without users getting involved. A minor security vulnerability could result in a major system exploitation, with devastating consequences.

The following are specific threats to PC users, in no particular order:

**Identity Theft** such as theft of character, social security number, medical, driver’s license, and credit continues to be a growing problem for both computing and offline world.

**Phishing attacks** designed to gather confidential information such as usernames, credit card information, passwords, account information, and other personal information, by spoofing a “trusted” entity.

**Malicious software** (“malware”) attack is another threat that faces today PC users. Malware includes computer viruses, worms, Trojan horses, rootkits, spyware, adware, keystroke logger, and other unwanted software. This software infiltrates a PC without user’s knowledge and usually collects, transmit, or process information on a target user’s computer.

**Botnets** is another security threat facing today’s PC and Internet users. Botnets is a collection of software robots (“bots”) that run autonomously and automatically. Computers that are not appropriately protected are easily “recruited” to become part of the botnets or “zombie computer.”

**Unencrypted files and data** is another serious threat to consumers. Imagine a PC that is used in preparing or storing personal and confidential information such as tax returns, medical records, financial records, loan application information, or banking information without data encryption. Unless the data stored in the PC is encrypted, the data can easily fall in wrong hands and compromise the confidential information contained in the system.

**Data loss** is a security threats to consumer. When was the last time you backed up your computer data? When was the last time you tested your backup procedure to make sure that your process works in the event of an actual need to restore data? Some of us have used our systems for years; and since our systems haven’t crashed, we see no need to save our data.

**Software, system, and application vulnerability** is another threat facing PC users. Most computer attacks take advantage of weakness in software, application, and operating systems, to succeed. Unless software manufacturers continue to release well tested and secured systems, avenues for computer exploitation will continue to evolve.

**Mobile or PDA attack** is another security threat vector that PC users have to worry about. Computer users are deeply intertwined with all kinds of electronic gadgets. If stolen or compromised, these devices can provide valuable information for an attacker to launch other target attacks against users.

**Social engineering threats** present another area of concern for personal computer users. Hackers and adversaries continue to use “typosquatting” (or URL hijacking) or phishing technique to attempt to steal information from users or distribute or infect users with malware.

**Wireless network** is another area of threat posed to the PC users. PC users may be connecting to a rogue/spoofed access point (AP) which will attempt to gather information from the user. Further, an innocent PC user may connect to an open wireless network and may get compromise by hackers lurking in the wireless network. Finally, a PC user may not adequately protect its own wireless network, leaving itself open to attack.

**Rogue/Hostile websites** is another area of security threat to the computer users. Hackers and malicious web site operators have set up sites to lure victims and compromise the machines visiting the sites. Rogue websites could be a spoof of the real website, which is designed to solicit confidential information from users.

**Computer users (People)** are a major threat to personal computers. Users of computers make it possible for social engineering attacks to occur. – whether, it is clicking on email links, downloading attachments, or providing personal information in an insecure manner. Without human involvement in the information transmission and sharing process, most attacks against PC would not occur.

**Lack of knowledge about security** is a threat. PC users do not have ready access to information relating to security without reading books or researching the topic on the Internet. The truth is that, most users generally have no interest in reading about security unless there is a virus outbreak or they have been compromised.

**Improper retirement or disposal of storage media** is another area of threat to PC users. New computers are purchased each day. Old ones are either auctioned/sold off, donated to charitable organizations or given to family and friends. What happens to the data that we have been collecting for the past five years? What about the information that is stored in backup DVD, CD, tape drive, USB devices, or hard drive? Unless these devices are properly forensically erased and physically destroyed, you waiting to become a statistics.

## CAUSES OF ATTACKS

You may wonder what causes these attacks. As we discussed above, a combination of factors are responsible. Most

attacks are common because of a number of reasons – human and technical:

### USERS’ FACTORS *Users’ Gullibility*

In computing, users are usually too gullible and trusting, giving out information when not needed, thinking that it is done through a secure channel. In fact, one might argue that secretly sending your social security number in email or text message doesn’t provide you any more security than broadcasting it in a cable television network.

**Users’ Mentality, Attitude, and Myth**  
Too often I hear these phrases: “I am pretty secure...,” “Nobody knows about me...,” “I have nothing anybody wants...,” “My wireless network is encrypted...,” “I have firewall and anti-virus software...,” “I am sending you my social security number or bank account number to you on email... No one else would see it, so the information is secure...,” or my favorite phrase: “I/We have never been hacked...” My suggestion to the reader is to assume that someone is attempting to hack into your PC or home network as you are reading this article. Ask yourself: “What can I do to improve my PC or home network security today?”

### Users’ Carelessness

We are usually in a hurry to plug our new computer gadgets without performing necessary security checking or carefully reading before we click of open attachments. Most of us do not take the same care we would in the physical world by safeguarding our files and data. What about allowing house maids or repair technician in your home when you are not there and without logging off or turning off your computer. How about when sending off your computer to the manufacturer or technician with everything (hard drive) intact? 📍

### TECHNICAL FACTORS

Technical factors that contribute to the cause of security compromise include:

#### *Un-patched or Outdated Software/Application with Security Vulnerabilities*

Vulnerabilities in software and client applications used by PC users are source for security breaches waiting to happen. "SANS Top-20 2007 Security Risks (2007 Annual Update)" summarizes some of the culprits nicely.

#### *Weak System Configuration*

Most attacks occur because PC users do not know or follow best practices in making sure that restrictive security setting is enforced in the configuration of the system.

### PHYSICAL FACTORS

Physical factors involve making sure that access into the area where the computer is located is well protected. Laptops should be locked down or be within view at all times. Data storage devices and media should be tightly controlled, locked up, and securely disposed when no longer in need or use.

### STAYING AHEAD OF SECURITY THREATS

Attacks against computers will continue to occur. Unless you practice a good personal computer security hygiene, which will make it easy for an attacker to go after the next computer and leave yours alone, users will continue to be plagued with issues.

The security of a computer is not just about using the latest and most expensive anti-virus or firewall system. A small mis-configuration can render your whole security investment useless and can get you in deep trouble. Here are some measures to implement to minimize exposure:

### USER'S MEASURES

#### *Watch Your Surfing Habit*

- Be cautious of web links in web blogs and chat rooms
- Be careful about the information that you publish and download from social websites, such as YouTube, Facebook, MySpace, etc. A media clip published on a website can contain Trojan or avenues of attacking the visitor.
- Provide personal information to a site that you know and trust, with a privacy policy you agree
- Clean out your browser cookies, cache, and temporary Internet files frequently to erase your Internet traces

#### *Be Less Gullible and Trust No One*

Remember, anyone could claim that they are your family member – a spoofing attack

#### *Change Your Mentality and Attitude towards Security*

Assume that someone is hacking you as you read this article. Do not practice "security by obscurity" or do not assume: "I am totally anonymous on the 'net..."

#### *Use More Caution in protecting your PC*

Double-check everything before you connect, click, and dispose. Always assume that anything you store on or transmit from the computer will be under attack by an adversary

#### *Be Cautious of Social Engineering Attacks*

- Watch out for rogue wireless networks and stay away
- Express caution in reading emails, following links, and downloading attachment.
- Delete videos and images attachment that contain amusing or other contents

#### *Arm Yourself with Security Awareness*

Take a security awareness training course or read about security voraciously.

### Technical Measures

#### *Harden Your System Configuration*

By hardening, we mean following industry best security practices to secure the configuration of your system, including:

- Install the most recent and stable operating system, application, and software
- Update your system and applications with the latest service pack and security fixes
- Install intrusion monitoring software to alert you of attacks against your PC. Monitor intrusion attempts on your PC
- Secure system accounts:
  - Create a user account for each user of the computer, for auditing purpose
  - Rename the "guest" and "administrator" accounts. Disable the guest account after renaming it.
- Enforce good password policy:
  - Password-protect files and directories
  - Practice good password habits, following many published guidelines
  - Implement biometric or multi-factor authentication.
  - Avoid sending Passwords, PIN, credit card numbers, social security numbers, etc. in an encrypted medium
- Secure your PC if it needs to be online. Enable screen saver with password-protection
- Install only applications and software that you absolutely need. Remember, each software and application is an avenue of security vulnerability.
- Disable file sharing

#### *Install and Enable Firewall*

Configure/enable firewall to block incoming, and in some cases, outgoing connection. Blocking outgoing connection is important as well to prevent some Trojan or malware that may need to call "home" upon successfully exploiting your system. ➤



# TOO HOT

# FOR SPOT!

## In hot weather, leave dogs at home.

On a 78°F day, the temperature inside a shaded car is about 90°F, while the inside of a car parked in the sun can reach 160°F in minutes. Even opening windows or parking in the shade won't prevent a dog from getting overheated. The heat is especially hard on dogs because

they can only cool themselves by panting and by sweating through their paws. With only hot air to breathe, dogs and other animals can suffer irreversible brain damage and even die of heatstroke in just minutes. This summer, leave your dog safe at home.

To learn more about helping animals in hot weather, please visit [HelpingAnimals.com](http://HelpingAnimals.com).

**PETA**

#### Install and Enable Content Filtering software

This includes software that filters and removes indecent content from being accessed or ran – anti-virus, anti-spyware, anti-malware (fights against Trojans and rootkits), etc. Configure your filtering software to automatically check for new updates and signatures. Manually scan your PC for malware at least once weekly.

#### Have an Independent Security Consultant Assess Your PC or Network Regularly

Having a reputable network security company evaluate the security of your system proactively can measure whether your system can withstand some attacks against your PC and users.

#### Secure Your Wireless Networks and Watch Out for Free/Rogue WiFi

Make sure you enable strong encryption and control access to systems that are authorized to connect to your wireless network. Any machine – whether wireless-enabled or not – needs to be configured securely before connecting it to the wireless network. Be careful when you connect to wireless network belonging to others to avoid compromising your own PC.

#### Secure Your Internet Browser

Configure your Internet Explorer, Firefox, or other browser securely. Mobile and hostile codes like JavaScript, and ActiveX controls attempt to exploits weakness in user browsers in order to compromise a PC. Update your browser constantly.

#### Encrypt your Data and Files

Encrypt your data and files that are stored and transmitted. Tools such as PGP ([www.pgp.com](http://www.pgp.com)) has a self-decrypting archival mechanism. WinZip ([www.winzip.com](http://www.winzip.com)) has a password-protection to encrypt your file. TrueCrypt ([www.truecrypt.org](http://www.truecrypt.org)) is another encryption software to use.

#### Backup Your Data and Files Proactively

To avoid potential lose or compromise of data, perform frequent data backup to CD/DVD, external hard drive, USB, etc. into two separate media and store these in separate locations. I would recommend first encrypting the data before backing them up. Store the backup media off site and test recovery often.

#### Forensically/Securely Erase and Destroy Storage Media

If you no longer need the data stored in a media, securely/forensically erase the media, verify that it has been erased, and then physically destroy the media. Your privacy can be protected in an attempt to recoup \$18 from selling your old disk!

### Physical Measures

#### Physically Secure Your System

Measures here include:

- Powering off your system when not in use
- Physically secure your systems – lock up laptops or desktops.
- Restrict access to PC location.
- Securing the storage devices – DVD, CD, USB, backup tapes, external hard drives, etc.

### CONCLUSION

In this article, we looked at the human and technical threats facing PC users as well as proactive preventive measures that can be implemented to stay ahead of the curve. Effective security measures call for “belt-and-suspenders” approach. When the factors suggested in this article are implemented proactively, your PC would be able to withstand common and casual attacks – causing the adversary to go after the next target. **PC**

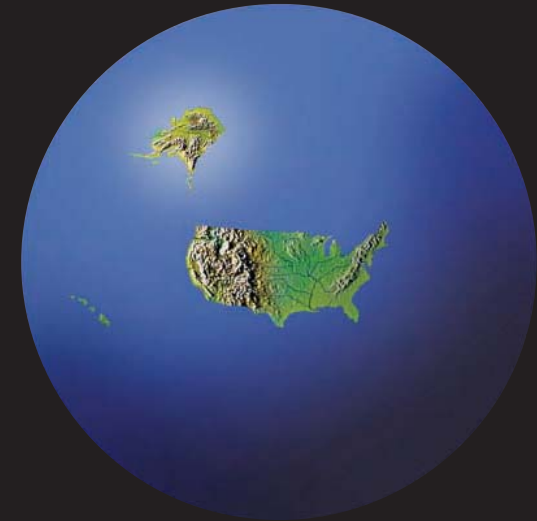
#### ABOUT AUTHOR:

*Inno Eronaba, CISSP-ISSAP, ISSMI, CISM, CISA, CHFI, is Chief Forensics Investigator with NetSecurity Corporation. NetSecurity provides digital forensics, hands-on security consulting, and Hands-on How-To security training solutions that are high-quality, timely, and customer-focused. For more information go to [www.netsecurity.com](http://www.netsecurity.com) or call 703-444-9009 or toll free at 866-664-6986.*

#### REFERENCES

The following references were researched in the writing of this article and provide a good source of information:

- CERT Home Computer Security, <http://www.cert.org/homeusers/Home-ComputerSecurity/>
- Microsoft guide for protecting PC users: <http://www.microsoft.com/protect/default.aspx>
- SANS Top-20 2007 Security Risks (2007 Annual Update), <http://www.sans.org/top20/>
- FTC's Identity Theft Resources: <http://www.ftc.gov/bcp/edu/microsites/idtheft/>
- Cryptogram: Safe Personal Computing: <http://www.schneier.com/crypto-gram-0105.html#8>
- Securing Your Web Browser: [http://www.cert.org/tech\\_tips/securing\\_browser/](http://www.cert.org/tech_tips/securing_browser/)
- Securing your Wireless Network: [http://www.practicallynetworked.com/support/wireless\\_secure.htm](http://www.practicallynetworked.com/support/wireless_secure.htm)
- Improve the safety of your browsing and e-mail activities, <http://www.microsoft.com/protect/computer/advanced/browsing.aspx>
- Reporting Computer, Internet-Related, or Intellectual Property Crime: <http://www.cybercrime.gov/reporting.htm>
- Wiki: <http://en.wikipedia.org/wiki/>



We are not alone.

There's a wonderful world around us. Full of fascinating places. Interesting people. Amazing cultures. Important challenges. But sadly, our kids are not getting the chance to learn about their world. When surveys show that half of America's youth cannot locate India or Iraq on a map, then we have to wonder what they do know about their world. That's why we created MyWonderfulWorld.org. It's part of a free National Geographic-led campaign to give your kids the power of global knowledge. Go there today and help them succeed tomorrow. Start with our free parent and teacher action kits. And let your kids begin the adventure of a lifetime.



**MyWonderfulWorld.org**

A National Geographic-led campaign

It's a wonderful world. Explore!