Avoiding

This week we’re going to discuss methods for keeping malware, viruses, trojans, key-loggers and other evil things from being installed on your computer.

We’re NOT going to discuss removal of these things. That’s another topic.

Discussion Topics

- (briefly) – Anti-virus programs
- (briefly) – Malware detection programs
- Tips for Safe Browsing Habits
- Malware Checking Sites
- Final Thoughts

Antivirus Software

Modern computer operating systems are already fairly well protected. It doesn’t hurt to install a third party antivirus program. In most cases, it isn’t necessary

If you need a program to remove a virus, it is already to late.

At some future date, we’ll compare antivirus software.

Anti-Malware Software

As with virus software, modern computer operating systems are already fairly well protected. It doesn’t hurt to install a third party programs. In most cases, it isn’t necessary

If you need a program to remove a malware, it is already to late.

Safe browsing habits are usually more effective.

Safe Browsing Habits

Update – Update - Update

- Operating Systems
- Browsers
- Firewalls
- Antivirus and Malware programs if you use them

Use Plain Old Common Sense

If you have a hunch a site is bad, it probably is.

Never download a file you didn’t search for.

Block Pop-ups

1) Pop-ups easily install malware
2) Evil web designers design pop-ups for easy accidental clicking
3) Most modern browsers have a setting to block them

Use a Firewall

Block unwanted intrusions into your system. Remember, the objective is to keep the malware out.

Use Bookmarks For Important Sites

Prevents you from accidentally going to an incorrect site.

It’s easy to make a tpyo and go to a spoofed site.

Use More Than One Browser

For example, having a browser you use only for financial sites greatly reduces the chance of malware infestations. Sites can be programmed to view your history.

If you must go to “dicey” sites do it with a separate browser.

Limit Your Browser Extensions

Beware of newer extensions.

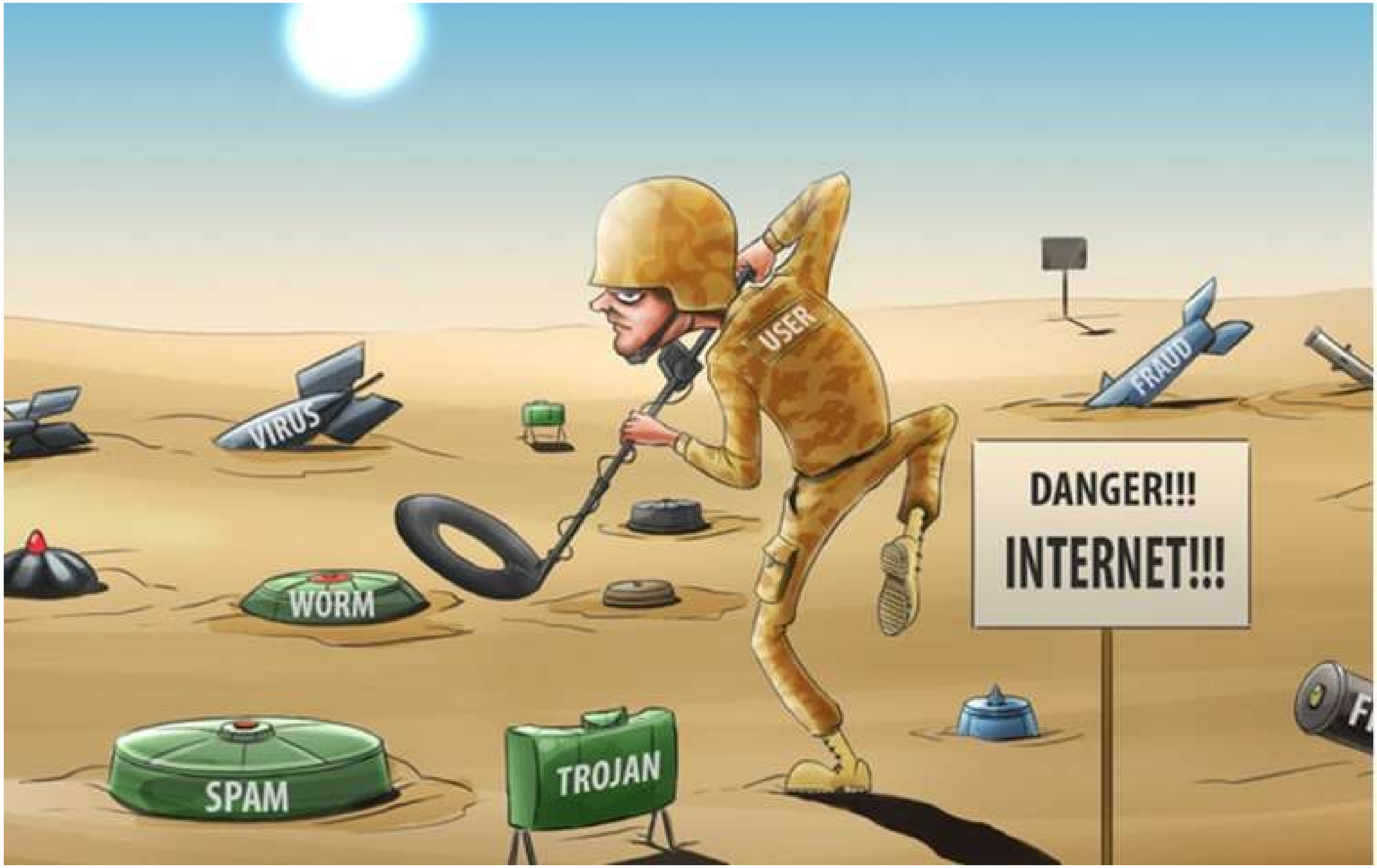
Browser extensions not only slow you down, it is an easy method for evil players to get access to your computer.

HTTPS vs HTTP

1) Data is encrypted
2) Designed to prevent hackers from accessing critical information
3) Domain ownership is validated by independent third parties

Remember, while domain validation is useful, it doesn’t say anything about the legitimacy of the owner.

Is That File Safe?



Malware Checking Sites

Like most things on the internet, there are thousands of sites where you can check files for malware.

Most are safe to use.

Don’t share any files you don’t want the whole world to know about!

Check Files & Links for Malware

1) Scan with your installed anti-malware programs.
2) Do an Internet search of the file name. If there is a problem, someone has finally found it.
3) Do the same if you’re not sure of the site you downloaded it from.
4) Check it on the sites listed on the next slide.

Sites To Help You Avoid Malware

- **Virus Total** – checks files and URLs with many scanners.
- **Online Link Scan** – checks URLs.
- **URLscan** – recent scans are sometimes interesting.
- **Quttera** – only scans complete websites. Can take a while.

Final Thoughts

- Trust your instincts
- Is the website with the file safe?

1) Do they have a real world address?
2) Is there a an e-mail contact?
3) Do they have a phone number?
4) Look for misspellings.

- Always use the the mouse rollover trick.

Next Week’s Topic

Staying Private Online

Unless someone has a different idea.

What’s The Next SIG Topic

Have you got a topic idea? Want to learn about something special? Tell me anytime you see me or contact me online.

clickers@tinys-bs.com

Clickers - General Discussion Google Group

All Presentations Available for Download

PDF Format

toxitman.com

Thats all
Folks