**Greenwich Library**

**HOW TO PROTECT YOURSELF FROM VIRUSES, WORMS, HACKERS, AND OTHER COMPUTER LOWLIFE**

Rich Malloy, Tech Help Today, 203-912-8268, malloy@techhelptoday.com

# Strong Passwords

## Must be long, at least 14 characters

## Include many different characters:

### Numbers, symbols, capital letters and lowercase letters

## Use random characters

## Avoid words, dates, names

# Is Your Password Strong?

## Password strength tests:

### www.grc.com/haystack.htm

### www.PasswordMeter.com

# *Tip:* Strong Passwords You Can Remember

## Pick a song lyric or sentence from a book

## Use the first letters of each word

## Include punctuation

## Example: 4Sa7ya,ofbfotc (“Four score and seven …”)

# Companies *Will* Be Hacked

## We can’t control that

## What does that mean?

## Different passwords for each account

# Password Manager Software

## Remembers passwords for you

## Creates complex passwords

## Enters passwords automatically

## Examples:

### LastPass

### 1Password

### Dashlane

# Biometric Authentication

## Reads:

### Fingerprint

### Facial pattern

## Convenient but secure

## Need password as backup

# 2-Factor Authentication

## Requires Two Things:

### Something you know: Password

### Something you have: Phone

# Which Accounts Need Strong Passwords

## Banking / Finance

## Retailers

## Email (can be a backdoor to other accounts)

# Phishing

## Fake Email or Web sites

## Tricks Internet users to reveal:

### Credit card, Social Security numbers, etc.

# Spear Phishing

## Targeted email

### Contains confidential customer details

# What to Do?

## Suspect *ANY* inbound message

### Email

### Pop-up

### Phone call

# Malware

## “Malicious Software”

# Types of Malware

## Viruses

## Worms

## Trojan Horses

## Ransomware

## Spyware

# Computer Viruses

## A program attached to a data file

## Spread when files are exchanged

### Email

### Downloaded songs and videos

### USB Flash Drives

## Requires user action to come alive

## Usually arrive as attachments

### May be disguised as Web hyperlinks

## Usually come from ***friends***

### Via your friend’s Address Book

# Worms

## Spread by themselves

## Through networks

# Trojan Horses

## Appears to be useful

### E.g., Removes viruses

## But does something bad

# What Does Malware Do

## Main purpose

### Spread to other computers

## Secondary objectives

### Slow down networks

### Display annoying messages

### Gain control of computers

### Destroy files

# Signs of an Infected PC?

## Odd messages or pop-ups appear

## Program icons suddenly are gone

## Browser takes you to strange places

## Computer is unusually slow

## Computer fan is very loud

## Antivirus programs stop working

# Ransomware

## The worst type of malware

## Encrypts your documents, pictures

## You have to pay ransom to decrypt

## E.g., “CryptoLocker”

# The Best Ways to Get Infected:

## Download free songs or videos

## Open strange email attachments

## Download free programs

## Share a USB Flash drive

## Go to porn sites

# Privacy & WiFi

# Email is *NEVER* Private

## If the Director of the CIA does not have private email….

## Then how can we expect it

# Spyware

## Transmits information about you

## Keylogger

### Records keystrokes:

### Passwords, Login IDs, etc.

# Who Uses Spyware?

## Bosses

## Hackers

## Parents & Spouses

# WiFi

## Wireless network in homes and companies

## Very convenient

## Not very secure

## Can be eavesdropped

# Wireless Eavesdropping

## Beware public places (Starbucks)

## Someone can “sniff” your connection

## Use https or a VPN

# The Internet of Things (IOT)

## Growing number of devices

## Minimal security

## Can spy on us

## Baby monitors have little security

# Laptop Webcams

## Can take pictures of you without your knowledge

## Put some tape over the camera when not in use

# Protection

## Antivirus Software for sale:

### Norton

### McAfee

## Free programs

### AVG

### Avast

### Microsoft Windows Defender

# Microsoft Windows 10

## Has Windows Defender

## Antivirus no longer needed

# “Zero Day” Virus

## Brand new virus

## Antivirus s/w can’t spot it

# Update Your Antivirus S/W

## Antivirus cannot protect you if…

### It does not know about new viruses

## Be sure software updates *automatically*

# Malwarebytes Free

## “Virus first aid”

## Quickly scans your PC

## Free, from malwarebytes.org

# If Your PC Is Infected …

## Scan with your Antivirus Program

## Scan with Malwarebytes

## Worst case:

### Reinstall your operating system and programs and backed-up data

# Update All Programs

## Be sure all programs are up to date automatically

# Go to the Source

## Update ***only*** at publisher’s site:

### microsoft.com

### adobe.com

### java.com

# Is Your Firewall Working?

## Test your PC’s vulnerability

### www.grc.com/ShieldsUP

# Set up Two Accounts on Your PC

## An Administrator account

### Use only when installing software

## A Standard User account

### Use this at all other times

# WiFi: Use a VPN

## VPN: Virtual Private Network

## Encrypts data point to point

## E.g., Tunnel Bear

# Which Files Should I Backup?

## Data files

### Files you’ve created or purchased

## Program files (less important)

# Where to Back Up

## External hard drives

### Connected directly to your PC

## Online (in the “cloud”)

# Check Your Backups

## Try to restore a random file

## At least twice a year

### When you change your clocks

Simple Solutions

# Are Tablets Immune?

## Mostly, yes

## Protected ecosystems

### Apple’s App Store

## But, hackers may soon invade

# Chromebooks

## Inexpensive

## Well protected

# Are Macs Immune?

## A few attacks so far

## But more viruses may come

## But you still need:

### Good passwords

### Be wary of Phishing attempts

### Data backup

# Summary

## “Convenient” is the opposite of “Secure”

## We can access the world — and the world can access us

## An arms race: Hackers only get smarter

## We have to be wary always

Checklists

# Checklist:

* Be wary of incoming messages
* Use good passwords
* Update your programs
* Backup your data files
* Be wary of WiFi networks
* Use a secure PC alternative

# Secure PC Alternatives:

* iPads and other tablets
* Chromebooks
* Apple Macintosh

# Checklist: Passwords

* Passwords are long and random
* Different password for each account
* Use a password manager

# Checklist: Data Backups

* External hard disk installed
* Set up cloud backup of most important files
* Check backups twice a year