

Speaker offers different view of technology

By John Weigle, Editor, Channel Islands PCUG

Jweigle (at) vcnet.com

Using humor, serious warnings and common sense, Bob Gostischa, the speaker at our March meeting, discussed "Technology from a Different Perspective."

Humorous photos and cartoons demonstrated some of the differences between today's youths and most members of the audience.

He noted that people today spend so much time looking at smartphones and tablets that they often don't know what's going on around them. His pictures included a couple in a restaurant texting each other rather than talking to each other; a Thanksgiving dinner at which everyone was using a smartphone, tablet or another device, and a baby playing with a smartphone. Customer service techs are getting younger and younger, he said, adding, "If I have a problem with my smartphone, it's my grandson that takes care of it."

He showed another picture of how bathrooms have changed. They used to be marked Men and Women; now they're Men, Women and Selfies, he said.

Gostischa said that when he is host of an event at his home, he has a basket at the front door and tells everyone to put their smartphones and tablets in it because they've come to visit. People who are there just to use his Wi-Fi can go home and use their own, he said. "Now we actually have visits that are meaningful visits," he added.

Today's "exercise" (texting) works on the brain, thumbs and fingers, "and the rest of the body leaves something to be desired," he said.

Turning more serious, Gostischa, whose presentations are paid for by Avast (travel expenses, lodging, food), which makes security software, said that no anti-virus program is perfect. The viruses come first, and the protection comes after anti-virus writers can examine the new code and update the anti-virus software. Computer users must be careful about what they do and not expect software to protect them from every threat all the time.

He introduced the cause of many technology problems, PEBKAC, which stands for Problem Exists Between Keyboard and Chair. "You are your biggest problem when it comes to the infection of your computers," he said.

Identity theft

Discussing identity theft, he said that when T-Mobile was hacked, it offered two years of free Experian credit watch. What they didn't say was that T-Mobile and Experian are parts of the same company. "One part of the company gets hacked, and the other part is going to make sure you're safe," he commented.

"It almost sounds like Uncle Sam."

Life Lock, which advertises heavily, doesn't really do much to keep identities from being stolen because nobody can do that. The company also doesn't do much to help those whose information has been stolen, he said. Basically, its customers are buying an insurance policy to help pay for the costs of straightening things out. The company recently paid \$100 million to the FTC because what it advertises and what you get are two different things, he said.

Scams and phishing

Scams and phishing attempts are common, he said. "We run into them almost daily." Good spam filters eliminate lots of scams, but users still must be careful of clicking on links in emails, on websites and in pop-up ads, he emphasized. If there is a descriptive link (one that doesn't show a URL but just says click here or something similar), you can determine the URL by hovering your mouse over the link, he said. Users who click such links and provide the information asked for give crooks enough information to empty their bank accounts. Legitimate companies that contact you will say to sign in to your account, not "click on this link."

Gostischa also added that no matter what a message on the Internet says, Bill Gates will not put money in your account if you share a post. And Microsoft will never call you to say it has discovered a virus on your computer and will, for a charge, remove it for you. Besides taking your money, the callers will usually add malware to your computer while pretending to fix it. If you get such calls, just hang up, he said. "I personally like to keep them on the phone for an hour and a half and waste their time," he added.

Eight clues suggest that your identity has been stolen, Gostischa said:

- Bank withdrawals you didn't make.
- Bills that you expect don't arrive.
- Merchants aren't taking your checks.
- You get calls from debt collectors about loans you never made.
- Your credit reports have unfamiliar charges and loans.
- You receive bills from health providers for visits you never made and doctors you never heard of.
- You can't get health insurance because of illnesses you don't have.
- You get an IRS notice that you filed more than one tax return.

One solution if you have all the credit you currently need, he said, is to freeze your credit. That prevents anyone from opening new accounts or getting new loans in your name. (Of course, if you apply for credit, you'll have to remember to unfreeze the accounts until your request is granted or denied.) You can do that through any of the credit bureaus for \$5, he said.

Crooks, he said, "may still steal your identity, but what good is it if they can't and in pop-up ads, he emphasized. If there is a descriptive link (one that doesn't show a URL but just says click here or something similar), you can determine the URL by hovering your mouse over the link, he said. Users who click such links and provide the information

asked for give crooks enough information to empty their bank accounts. Legitimate companies that contact you will say to sign in to your account, not “click on this link.”

CryptoLocker and its variants

CryptoLocker and its variants are another threat, Gostischa said. Hollywood Presbyterian Medical Center was infected and had no choice but to pay \$37,000 for the key to unencrypt its files. CryptoLocker and its variants encode all the files on the infected computer and can also branch out to any devices attached to the computer — hard drives, flash drives, and networks, Gostischa said. Owners of infected computers get a message that demands a ransom payment within a few days and a warning that the key to open the files expires in a short time, and once it's gone the files can't be unencrypted.

The only real defense — short of never going to the Internet or connecting to any other device — is regular image backups, Gostischa said. He uses the Windows backup tools every Sunday, but third-party programs are also available. An image backup copies everything on the drive, including the operating system, programs, data, music, pictures, preferences and the registry.

He suggested making regular image backups on an external hard drive and, when the backup is completed, unplugging the drive from the computer and the wall power so it can't be infected before the next backup.

A new variant encrypts the Master Boot Record, he said.

So far, CryptoLocker malware has not been written for Apple and Linux systems, but that will change, Gostischa predicted.

The biggest loss from CryptoLocker attacks is the user's personal information because, even though it's time-consuming, the operating system and programs can be installed on a new drive.

Victims of identity theft, he said, should report it to www.idtheftcenter.org and <https://www.identitytheft.gov> or <https://www.consumer.ftc.gov/topics/identity-theft>. He recommended getting free credit reports every quarter by using Equifax in January, Experian in May and Trans-Union in December. By law, everyone is allowed one free report from each company each year.

Who are you dealing with?

Internet users often assume that people they're talking to are really who they say they are, but that's not always true, Gostischa said.

Social engineering is a common way that crooks use to try to get people to do something that will infect their computer, he said. One scam says Bill Gates will put \$5,000 in your account if you will share the message.

He also urged users not to like posts on Facebook unless they're from people they know from face-to-face contact.

Given the dangers, people should be quite careful about giving out personal information or making appointments to meet each other, he warned. "These people are out for money," he added.

Another precaution is to be sure both sides of a texting conversation are talking about the same thing, a point he illustrated with this joke:

"On a cold winter morning, while her husband is away on business, a wife has a problem at home and sends a text message to her husband: 'Windows frozen, won't open.'

"Husband texts back: 'Gently pour some lukewarm water over it, and gently tap the edges with a hammer.'

"Five minutes later, wife texts back: 'Computer really busted now.'"

On another matter, he emphasized, "When you make Facebook friends, you're sharing your information and your friends'."

Free programs recommended

Gostischa recommended several free programs that he said everyone should have. He lists a batch of others at <http://goo.gl/5v4slQ>. The entire list is in a separate box on the next page.

Some of his general comments on the programs follow:

Unchecky unchecks what you don't want checked when you install programs or updates. clear what's being installed. Using the custom installation lets users pick and choose what gets installed.

Malwarebytes should be used as an adjunct to any anti-virus program, he said. Malwarebytes does not detect viruses but other forms of malware, including potentially unwanted programs that piggyback on some programs. Users should not have more than one anti-virus program because they can conflict and slow a computer down, but other anti-malware programs are not a problem, he said.

CCleaner empties the recycle bin and deletes some other things. He said that leaving the default setting for registry cleaning should not create any problems. Users can make a computer unbootable by editing the registry. Cleaning the registry does not noticeably speed up a computer, he said.

WinPatrol monitors changes to computers, especially the installation of new programs. It also monitors registry changes. Gostischa has arranged a 50% discount price for the paid version for those who enter "bobsfriends" when ordering it at

<https://www.winpatrol.com>. Click on the hamburger menu (three horizontal bars) to see all the company's products.

Although Avast has a password manager (Avast Passwords at <https://www.avast.com/passwords>), Gostischa uses LastPass as his main password manager, he said. Having two password managers provides a backup if one fails or is not available and is not dangerous. Be sure to write down the password for the password manager because it can't be recovered, he warned. Password managers store their data on the cloud.

Changing default passwords on modems and routers is also good protection, he said.

Avast also makes anti-virus and antimalware programs for phones and tablets, he said, emphasizing "They're not toys. They are miniature computers, and my smartphone is actually smarter than my laptop." The younger generation uses only these devices, which contain vast amounts of data.

He also urged anyone looking for apps for such devices to buy them only from the recognized app stores. Don't buy apps that the writer says aren't in the stores "because they don't like us."

An Avast anti-theft protection is also available that sends a message to the computer's owner when the device is activated and lets the owners set off a loud siren when they get the message. The siren is also a good way to find the device if you've misplaced it. Another feature lets users kill the device, but be sure it's stolen before using it, he said, because the action can't be reversed.

Another Avast product, Secure Me, lets users create a virtual private network (VPN) when using public Wi-Fi. Gostischa also emphasized that anything you put on the Internet is no longer private.

He also said he believes Apple could have helped the FBI hack the smartphone used by San Bernardino terrorists because he's never known a coder who didn't build in backdoors to programs.

Rebooting solves problems

A potential solution for many problems if a computer that has been running for some time starts doing strange things is to shut it down, disconnect it from the wall (if you have a laptop, remove the battery if you can), and let it sit for a while. Then connect power and turn the computer back on. The same technique works for routers, he said.

Recommended software

Gostischa recommended several free programs that he said everyone should have. He lists a batch of others at <http://goo.gl/5v4sIQ>, which has the links to all the programs, some of which are also on the CIPCUG flash drive. The entire list follows:

These are the programs recommended at the meeting:

Unchecky — To help prevent installing unwanted add-ons.

Avast! Free — To keep you safe on the Internet and protect your computer.

MCSHield — To protect you from infections on USB drives.

Malwarebytes Free — An excellent companion for Avast!

Ccleaner — To clean up leftovers when visiting the Web and using your programs.

LastPass — A password manager that lets you create, manage and safely store your passwords.

WinPatrol — To alert you of unexpected changes to your computer.

Glasswire — Although it was on his list, Gostischa said this program is for the true paranoid. It shows all the activity of your firewall, monitors network activity and reveals hosts that are known threats, unexpected network system file changes, unusual application changes, ARP spoofing, and DNS changes. Its website is <https://www.glasswire.com/>

These are the other items listed on the website mentioned above:

PC Decrapifier — Helps you delete all the useless programs that come prein-

stalled on that new computer.

SlimComputer — Free. Helps identify software that comes pre-installed on a new computer.

Ninite — Makes adding new programs to your new computer a breeze.

Unlocker — Helps bypass “Program is in use” message when trying to uninstall a program.

Recuva — Helps recover something you deleted in -error.

Classic Shell — If you’re using Windows 8.1 and want your Start Menu back, this is what you need.

VLC Media Player — An excellent Media Player that also gives you back the ability to Play DVDs in Win. 8.1

Paint.net — An excellent Graphics program. Photoshop for the average user and, it’s totally free.

Nitro PDF Reader — Safer than Adobe. It’s free and also allows you to create PDF files.

CutePDF — Convert most items into a PDF file via a printer driver.

Cloud Storage — Storage on remote servers for pictures, files, videos, etc. (Google Drive, Sky Drive, Dropbox, Amazon, Box, etc.)

A productivity suite — If you can’t afford Microsoft’s Office, try Kingsoft Office, OpenOffice or LibreOffice.

7Zip — A compression tool to work with zip, rar, iso and most other compressed files.

Driver Booster — Free. An excellent utility to keep your drivers updated.

EaseUS Todo Backup — Free. An excellent program to create reliable backups including Image backups.

The following are listed on website as

Other Free Software to consider:

Free Imaging Software for creating System Image Backups: 1-Click Restore, free, http://www.keriver.com/oneclick_free.html; Drive Image XML,

<http://www.softpedia.com/get/System/Hard-Disk-Utils/DriveImage-XML.shtml>; and Clonezilla, <http://clonezilla.org/downloads.php>.

Prevent CryptoLocker from installing: <http://www.foolishit.com/vb6-projects/cryptoprevent/>

Should I Remove it — <http://www.shouldiremoveit.com/download-thankyou.aspx?download=1>

Herd Protect — <http://www.herdprotect.com/downloads.aspx>

(BootSafe) — An easy way to get to Safe Mode: <https://goo.gl/RXgKCO>

Windows 8 App Remover — <http://sourceforge.net/projects/windows8appremover/>

Free Firewall programs: Comodo Firewall — <http://www.comodo.com/home/internet-security/firewall.php>;

TinyWall 2.1 — For Win Vista, Win7 and Win8: <http://tinywall.pados.hu/>

AdwCleaner is a tool that deletes Adwares (software ads), PUP/LPI (Potentially Undesirable Program),

Toolbars, Hijacker (hijack of the browser’s homepage). Download link: <http://general-changelog-team.fr/fr/downloads/finish/20-outils-de-xplode/2-adwcleaner>.

FileHippo.com — Update checker helps you keep your installed programs up-to-date.

Online virus/malware checkers used to double check when you suspect a false positive (links on the site).