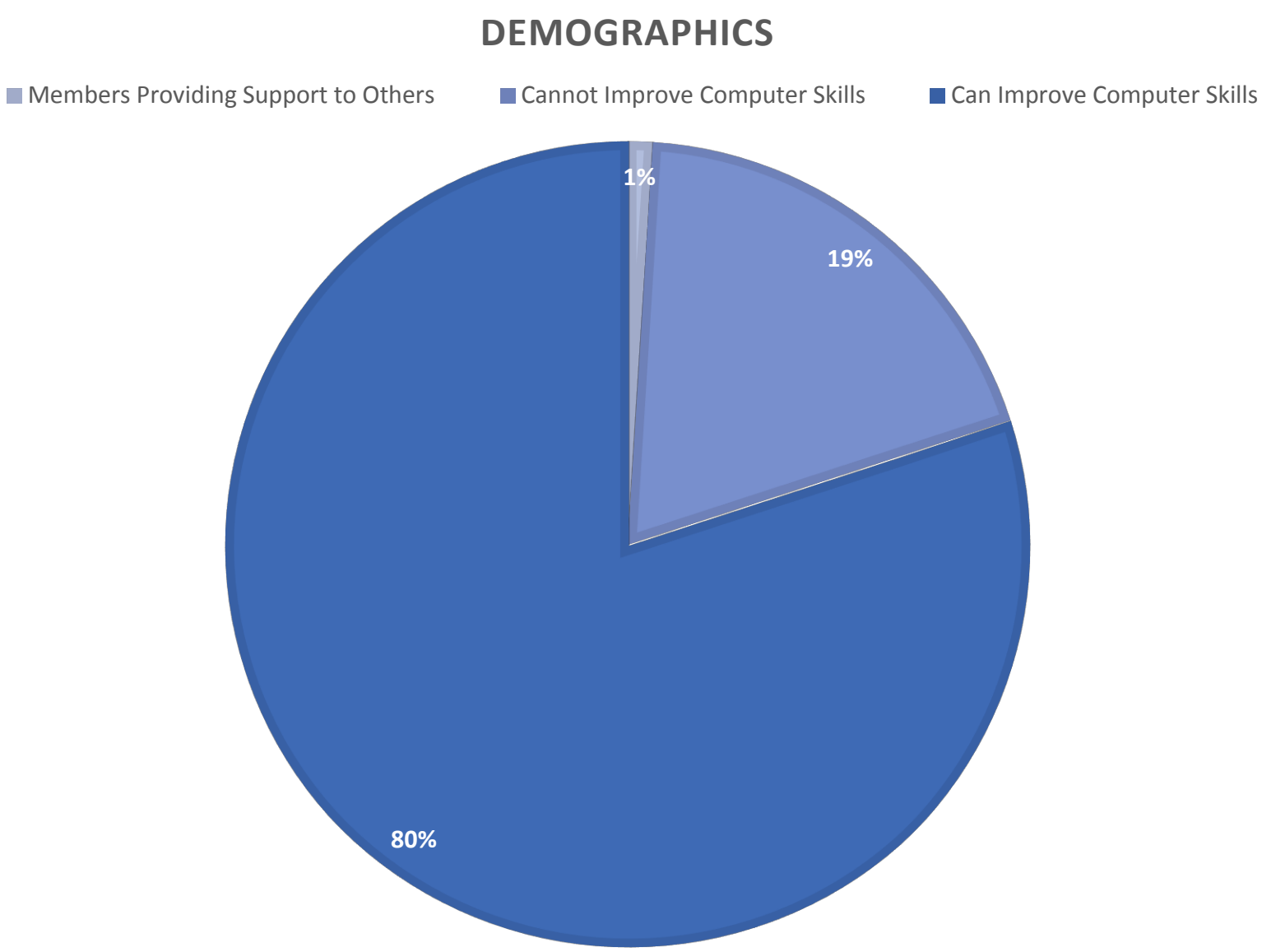
How Not To Get a Virus
&
What To Do, If You Do!

Ballroom - 021014

SCTXCC Membership



Forward

- I do not believe that a User can ever experience the benefits of computer usage unless and until you acquire the ability to resolve basic computer issues for yourself!

- “Murphy’s Law” definitely applies to computer usage

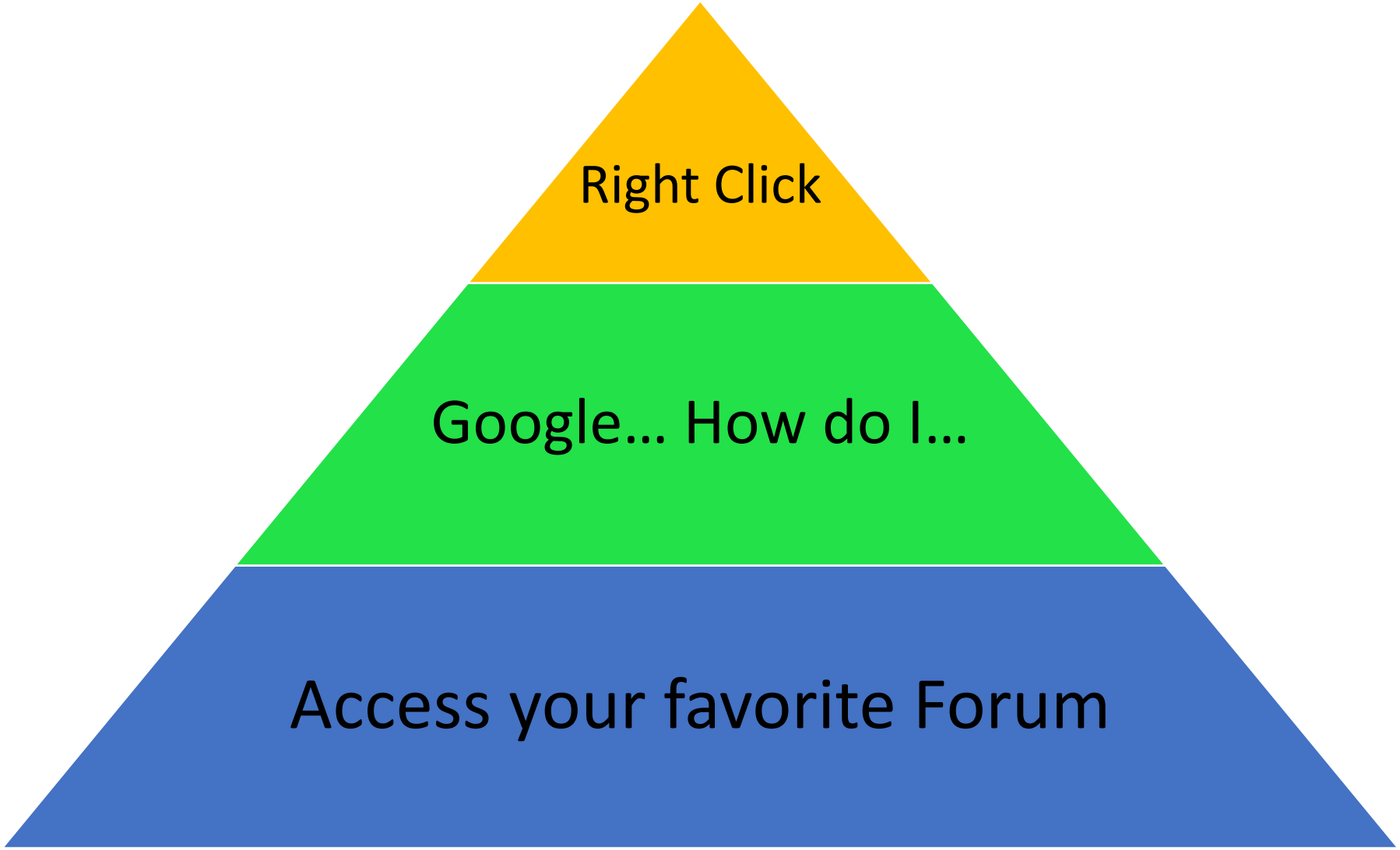
- If you do not understand, embrace and practice the fundamentals of computer problem solving, the computer will be a continuing source of frustration, rather than an effective tool

- Basic computer problem solving requires no little or no technical knowledge, all that’s required is to understand the process and it’s simple!

A Popular Misconception…

- It’s believed by some, that presenters and support people are “computer gurus”, geeks or some how more computer literate than other Members
- Truth is we are very much like each of you…
- We have acceptable computer skills with those things that we do frequently and very poor skills with things that we do infrequently
- It’s important to understand that computer ability is more about frequency than it is about knowledge!
- So, how then do you find out how to do what you don’t know how to do?

When You Don’t Know What To Do?



Malware

Forward

- 1st and foremost, it's important to understand that all operating systems and software by nature, are potentially unsafe and hack-able, it all depends on how they are used!
- 2nd there is no antivirus or spyware program that offers total protection
- Malware is evolving, becoming more sophisticated in its functionality and hackers are targeting "seniors", computers and mobile devices in new ways
- A leading malware vendor estimated that in 2013 there were 69 new pieces of malware PER MINUTE!
- Malware is a self inflicted wound and is something that you do to yourself and is preventable
- It is essential that Users understand the origin, prevention and or removal of malware.

Origin of Malware

- Malicious websites
- Employing “Webmail” as primary access to email
- Email, links & attachments
- Browser & add-on vulnerabilities
- Downloads from the Internet
- Out of date software
- URLs (links)
- User poor judgment

10 Indicators That Your Computer is Infected

- Unexpected Crashes:
- Slow System: it may be because your system is infected with a virus.
- **Excessive Hard Drive Activity**: is a warning sign of a potential infection.
- Strange Windows: pop ups.
- Peculiar Messages: dialogue boxes when your system is running alerting you that various programs or files won't open, is a bad sign.
- **Unintended Program Activity**: i**f you receive notification that a program is attempting to access the Internet without your command, this is a serious warning sign that you are the victim of malware.**
- **Random Network Activity**: if your router is constantly blinking, something might be wrong.
- **Erratic Email**: if you hear from your contacts that they're getting emails from you that you did not send , this is an indication that your account has been compromised (or that your email password has been stolen).
- **Blacklisted IP Address**: If you receive notification that your IP address has been blacklisted, consider this about as sure a sign as any that your PC is not in good hands
- Unexpected Antivirus Disabling: Many malware programs are designed to disable the antivirus suites that would otherwise eradicate them, so if your antivirus system is suddenly not operating this could be a sign of a much larger problem.

Best Practice:

- Systematically run e.g. Malwarebytes and SuperAntiSpyware, in "Safe Mode", to remove infections

Email Phishing

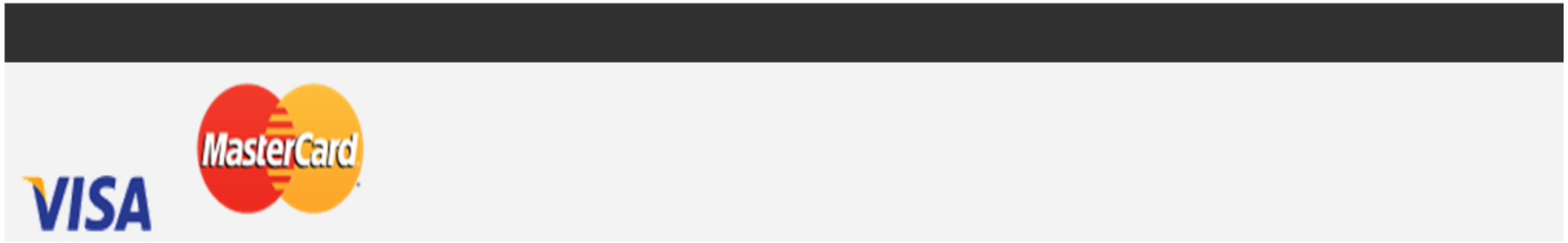
Thu 2/6/2014 8:45 AM

Visa / MasterCard <acdvzdaku@host2company.com>

ATTN: Important notification for a Visa / MasterCard holder!

To windows

Message windows_Account_Report_A7FA587751.zip (58 KB)

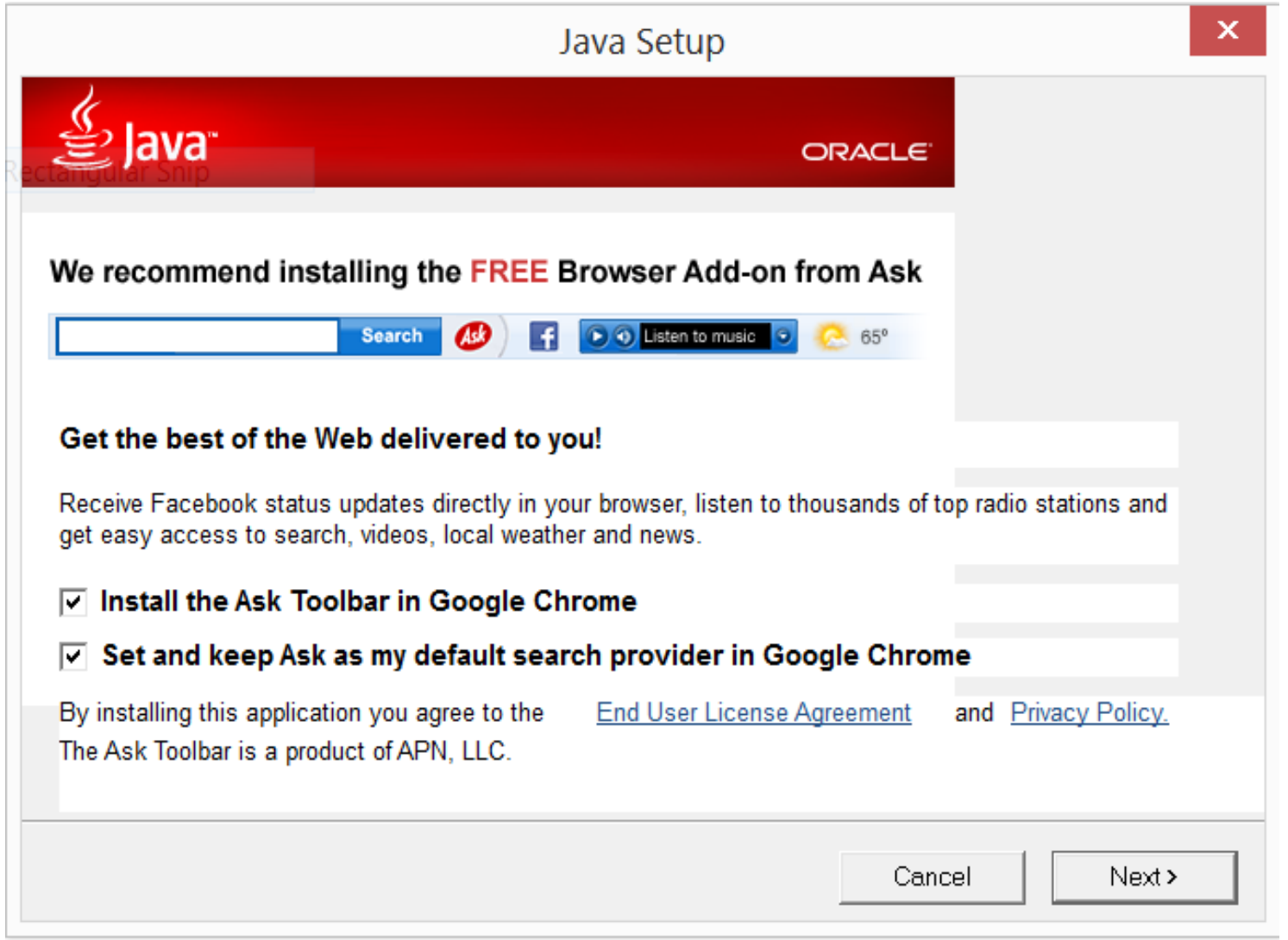


Important notification for a Visa / Mastercard holder!

Dear windows, Your Bank debit card has been temporarily blocked

We've detected unusual activity on your Bank debit card . Your debit card has been temporarily blocked, please fill document in attachment and contact us

Downloads With “Bundled” Add-ons



CryptoLocker Virus

Basic Malware Software Guidance

- One “real-time” antivirus program
  - There are “free” and for “a price” versions

- Two “real-time” spyware programs
  - Most antivirus programs also provide a spyware component
  - So, typically you need one additional spyware program
    - Malwarebytes or SuperAntiSpyware are good choices

- Web of Trust (WOT) is a web browser add-on and is recommended to give Users a heads up regarding “dangerous” websites

- At least monthly, run a “deep” scan with either Malwarebytes or Super Anti-Spyware, in “Safe Mode” (see Appendix for “how to” in Win7 & Win8.1
  - Remove all infections that these programs find

- Remember there is no antivirus or spyware program that will provide total protection!

Malware Prevention Best Practices

- Use “strong” passwords (Upper & lower case alpha, numbers & symbols, eight digits or more in length)
- Employ password management software
- Do no use webmail as your primary access to your email, employ an “email client”
- Install and pay attention to the guidance provided by Web of Trust (WOT)
- Slow down, read before you download to avoid unwanted software and or modifications to your computer
- Do not “wander” around the Internet or click on website links
- Only download software from reputable websites, slow down and read what you are downloading
- Do not ever click on any email link that requests personal information
- Have multiple browsers installed on your taskbar, employ the most current version, reduce the attack surface with minimal add-ons
- Backup, backup, backup and if you have really important stuff, consider the 3-2-1 back rule

Resource List

- Password management software
  - Last Pass: https://lastpass.com/
  - DashLane: https://www.dashlane.com/passwordmanager
  - Keeper: https://keepersecurity.com/download
- “Best” tools for malware removal, available from www.ninite.com
  - Malwarebytes
  - SuperAntiSpyware
- Web of Trust https://www.mywot.com/
- Best source for additional browsers (e.g. Chrome and Firefox) www.ninite.com
- Best website for “free” software www.ninite.com
- Best source for specific malware removal tools is Bleeping Computer (101 “tools”) http://www.bleepingcomputer.com/download/windows/
- SCTXCC Member Forum www.sctxcc.org
- SCTXCC Help Center, Tuesday afternoons and Saturday mornings in the Annex

Appendix – How to Access Safe Mode

- Windows 7, Vista & XP:
  - ✓ Boot or re-boot computer
  - ✓ Immediately, depress the F8 key, repeatedly
  - ✓ On the next screen, use the “arrow Keys” to page to “Safe Mode with networking”, then depress “Enter”
  - ✓ Be patient and you will be in Safe Mode

- Windows 8.1:
  - ✓ On the Start page or in the Search box type… advanced
  - ✓ When the search results appear click… Change Advanced Startup Options
  - ✓ Then under Advanced Startup click… Restart Now
  - ✓ Then click… Troubleshoot
  - ✓ Then click… Advanced Options
  - ✓ Then click… Startup Settings
  - ✓ Then click… Restart
  - ✓ Then on the next screen, depress the F5 key (Safe Mode with Networking)
  - ✓ Then provide the User Password if prompted, and
  - ✓ You will boot into Safe Mode with Networking