

A person is shown from the side, working on a laptop. The scene is overlaid with various futuristic digital graphics, including a large shield with a padlock, a globe, a bar chart, and a world map. The background shows a window with greenery outside. The overall aesthetic is high-tech and professional.

Keep Your Information Safe with These 15 Tech Tips

PRESENTED BY: MICHAEL MILLER, DIRECTOR OF OPERATIONS AT MGA

Agenda



Introduction



Top 15 Tech Tips



Q&A



Introduction

Michael Miller, Director of Operations at MGA

- My role within the Firm and how it relates to you
- Liaison between IT department (“techies”) and the end users
- Open forum – inquire/challenge/participate

Scary Facts

Did you know that three companies control 70% of the US media market?

- 70% of the social media market is controlled by Facebook & Twitter
- 71% of browser traffic is controlled by Google Chrome and their SEO

71% of cloud computing is controlled by AWS, Azure, and Google Cloud

45% of the global population have YouTube accounts, and it is localized in 91 countries and 80 languages.

Every aspect of the subscribers behavior is tracked and analyzed either for direct marketing or sale to others.

- Downloading apps on your phone – you are authorizing all your data and habits to be shared



Tech Tips

1. Updates

2. Enter your own URLs

3. Site safety

4. Virus notifications

5. Choose your flexible friend

6. Anti-Virus/Anti-Malware

7. Firewall

8. Secure your browser

9. Take control of emails

10. P2P/IM

11. Wireless security/public networks

12. Backups

13. Clean up after yourself

14. Attachments/downloads

15. Passwords

Computer Operating System

- Windows (Windows 10, 8.1, 8, 7, XP???)
- Apple (Mac OSX 10.15)

Anti-Virus/Anti-Malware

- Update Schedule (automatic)/Scan Schedule (automatic)

Smartphones

- Apple (iOS 13.3 – 12/10/2019)
- Android (10 – 9/3/2019)

Other Devices with Firmware

- Routers, IP Cameras, TV and DVD Players, Smart Appliances, etc.
- Apple Watch (6.1.1 – 12/10/2019)
- tvOS

Updates

Enter Your Own URLs

Suspicious email with a link?

- Think **FIRST**, click **LAST**
- Do you know the sender?
- Do you have an account with the entity it is referring to?
 - If so, open your internet browser and enter that URL directly, do **NOT** click on the link in the email.
 - Remember the “hover” test.
- How to see a link from your iPhone

Example:

- Email from “Chase” about activity on your account.
 - Visit Chase directly and do not click on any embedded links.


Site Safety

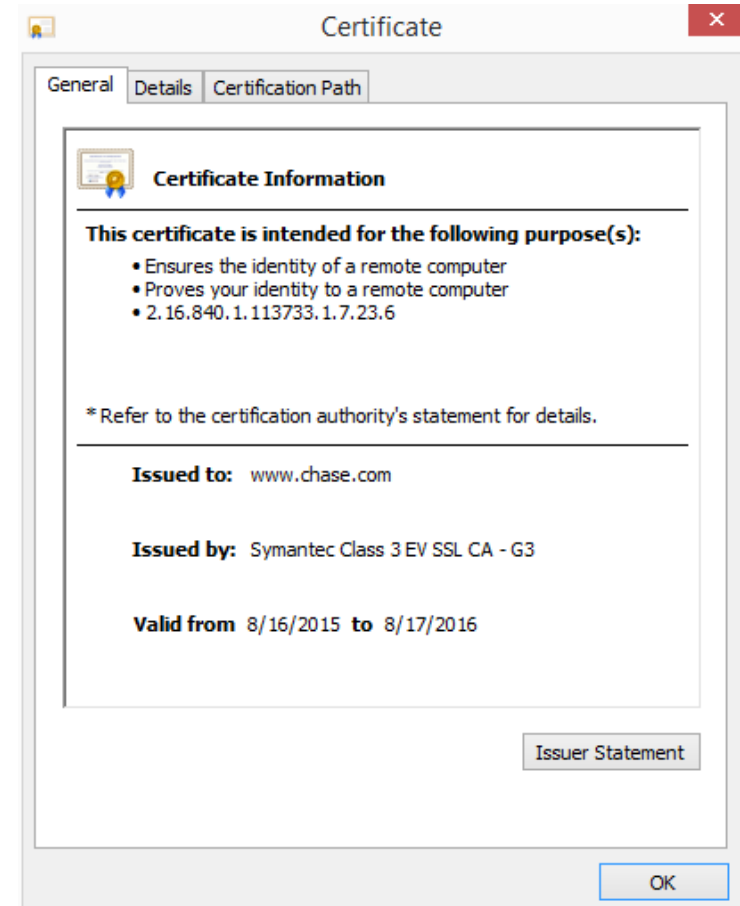
Entering private/confidential information?

Processing a transaction (i.e. purchase)?

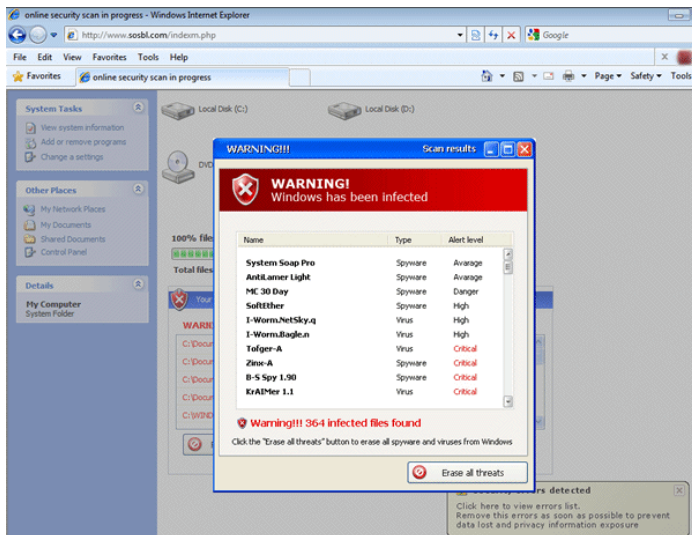
Safety check

- Make sure you are on a secure site
 - (https://)
 - But whose site are you on???

 JPMorgan Chase and Co. [US] <https://www.chase.com>



Virus Notifications (Fakes)



Virus Notifications (Fakes)

Steps to take

- Windows (launch task manager to end process)
- Apple (launch force quit to end task)
- DO NOT CLICK ON THE WINDOW
- Immediately run both Anti-Virus and Anti-Malware software and follow the queues given

Choose Your Flexible Friend

Purchasing on the internet?

- **Debit or Credit?**
 - Using credit card, there is a firewall between your bank account and the vendor.
 - Federal law that provides protections unique to credit cards.
 - When you purchase something on your credit card, a bank issuing the credit card makes the payment to the vendor. You are obligated to pay the bank only after you are in agreement that the charge is legit and that the item or service you bought was delivered as agreed.
 - Federal law and bank's policies include some protections from fraudulent or unauthorized transactions due to debit card theft. Before a questionable transaction is sorted out, the money is taken from your bank account.
- **Paypal and other shopping tools (i.e. Apple Pay or Visa Wallet) alternative can provide an extra layer of protection, if used correctly.**



Everyone should utilize both and ensure each is set to automatically update and automatically scan

Set ideal times to run updates and scans



Are you paying for this software?

Tips to get good solutions for zero additional out of pocket costs

Anti-Virus/Anti-Malware

Firewall

LOCK IT UP – EVERYWHERE YOU CAN

- Computer
 - Windows – Control Panel – Windows Firewall
 - Apple – System Preferences – Security – Firewall
- Internet Router
 - Settings vary by manufacturer
 - www.tomsguide.com – great resource

Secure Your Browser

Run the current version

Security settings

- Cookies – A little piece of information that is not only stored on your pc but on a website's server to remember you. Can include surfing habits, your approximate location, shopping habits, etc.
- Safety Zones
- Active X
- Plug-Ins

Toolbars

Take Control of Email

Spam Filters

- Use and train your computer/email provider to work more efficiently. Mark mail as junk or spam as applicable

Phishing

- Clever drafted emails attempting to get personal information (login details)
- Utilize the 'hover' test

Safe Unsubscribing

- Unsubscribing to the trove of marketing emails can be good – but be sure you do not subject yourself to phishing attempts. Remember to use the hover test or enter URLs manually.

P2P/IM

P2P (Peer to Peer)

- File Sharing, Torrents
 - Software can open ports on your network (create security breaches)
 - Client software can be buggy/infected with malware
 - Received files can include viruses or malware

IM (Instant Messaging)

- Malicious links or phishing attempts
- Beware certain ad-supported client software

Wireless Security/Public Networks

Wireless Security

- Your home wireless network should utilize current security standards (WPA2 is today's standard)
- Ensure that both your wireless SSID and your router are password protected

Public Networks

- When you are on one of these networks, your data can be intercepted
- Utilize guest networks
- Is streaming the Top 20 @ Starbucks worth putting your data at risk?
- Safeguards – VPN (encrypts all data from your device). Even though we have secure networks at home, don't overlook VPN value to truly mask your traffic.

Backups

Memories are now digital

If your house was burning, no longer are we grabbing the wedding album, we are grabbing our CPU!

Backups should be redundant and technology makes this cheap

- Local Solution (USB drives, Apple Time Capsule)
- Online Cloud Solution (Backblaze, Carbonite, ZipCloud, etc.)
- Due diligence on who you use

Clean Up After Yourself

Business Centers/Shared Computers

- Keep it “clean”
- Do not browse to websites where you would enter any usernames or passwords
- Safe Browsing Windows
- Clear internet cache/files when done

Attachments/Downloads

At this point you know the drill
(broken record)

Utilize good judgment

Who is the sender (and do they frequently send attachments)?

Is the content and language within character of the relationship?

Utilize Anti-Virus software to scan all downloads before viewing/installing/playing/etc.

Passwords

My thought is a password is only strong enough if you cannot remember it 30 seconds after creating it!

Vary your password from site to site

Utilize tough standards – different case, numbers, symbols, etc.

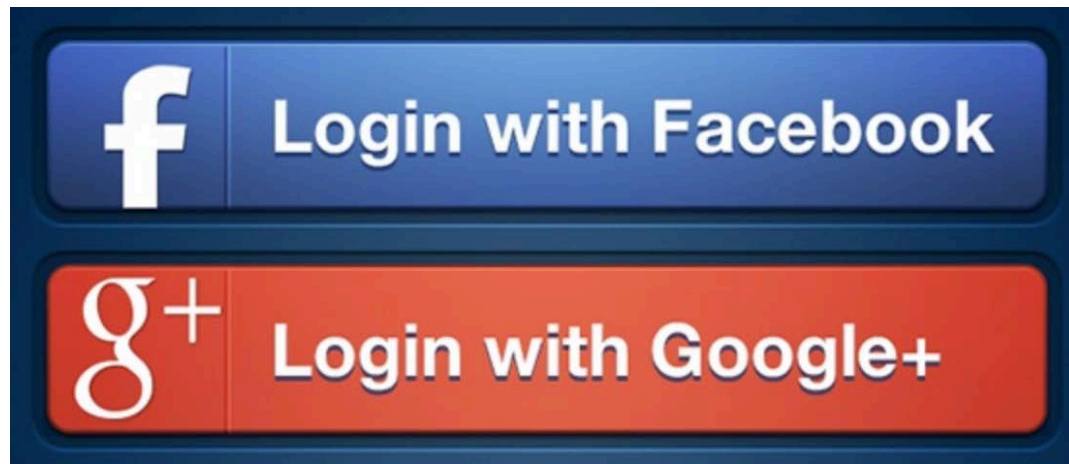
How do you keep it all straight?

- Utilization of SAFE apps (not a binder with “PASSWORDS” written down the spine)
 - SpalshID, 1Password, LastPass, RoboForm, etc.
 - Chrome Sync and Apple Keychain
 - Programs utilize high-level encryption to protect your information

Passwords

What happens when you log into websites with your Google or Facebook accounts?

- You're relying on Google or Facebook's security
- What type of access are you giving them to your accounts? What data are you allowing to be shared?
- Take back control - you can manage the sites you are currently using via your Google or Facebook settings



Insurance and Other Cool Tools

Cyber insurance

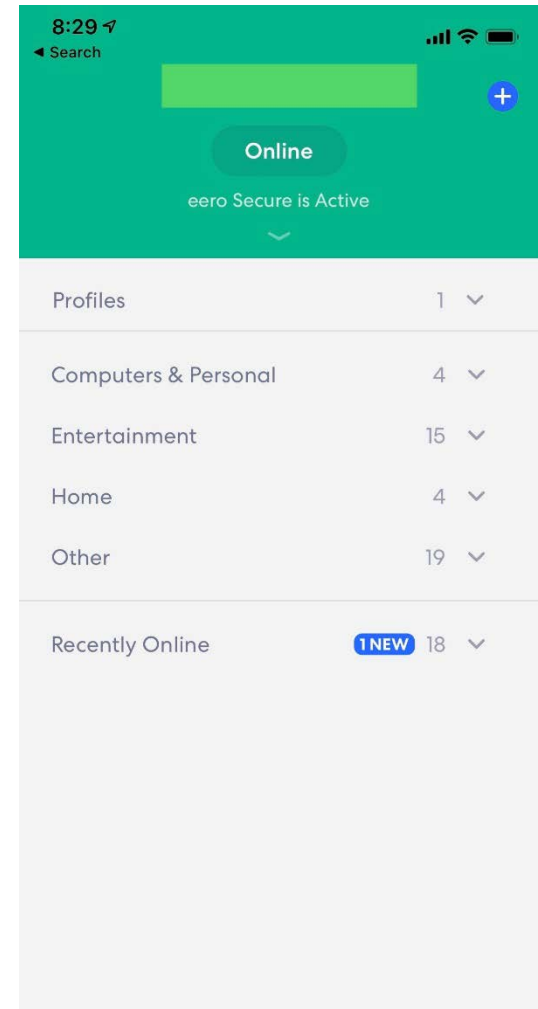
Anti-phishing tools (Knowbe4)

Router-based /cloud-based security add-ons (eero Secure, Circle, Netgear Armor, etc.)

- Screenshot from eero Secure shows 50+ devices on the internet from one home router. What is it doing? Is it safe?

Personal identity protection

Segmented guest networks



MICHAEL MILLER
MMILLER@MGALLP.COM
WWW.MGALLP.COM

QUESTIONS?