INTERNET

SECURITY FOR

SENIORS

1

Your Presenter

- Education:
    - BSIT – Information Technology
    - MAEd – Adult Education

- Employment:
    - Retired US Navy Chief Petty Officer
    - Microsoft Tech Support
    - Muscular Dystrophy Assn.
    - Tucson VA Hospital

- Volunteer
    - Web Director, Computer Booters - Sun Lakes
    - APCUG Speakers Bureau
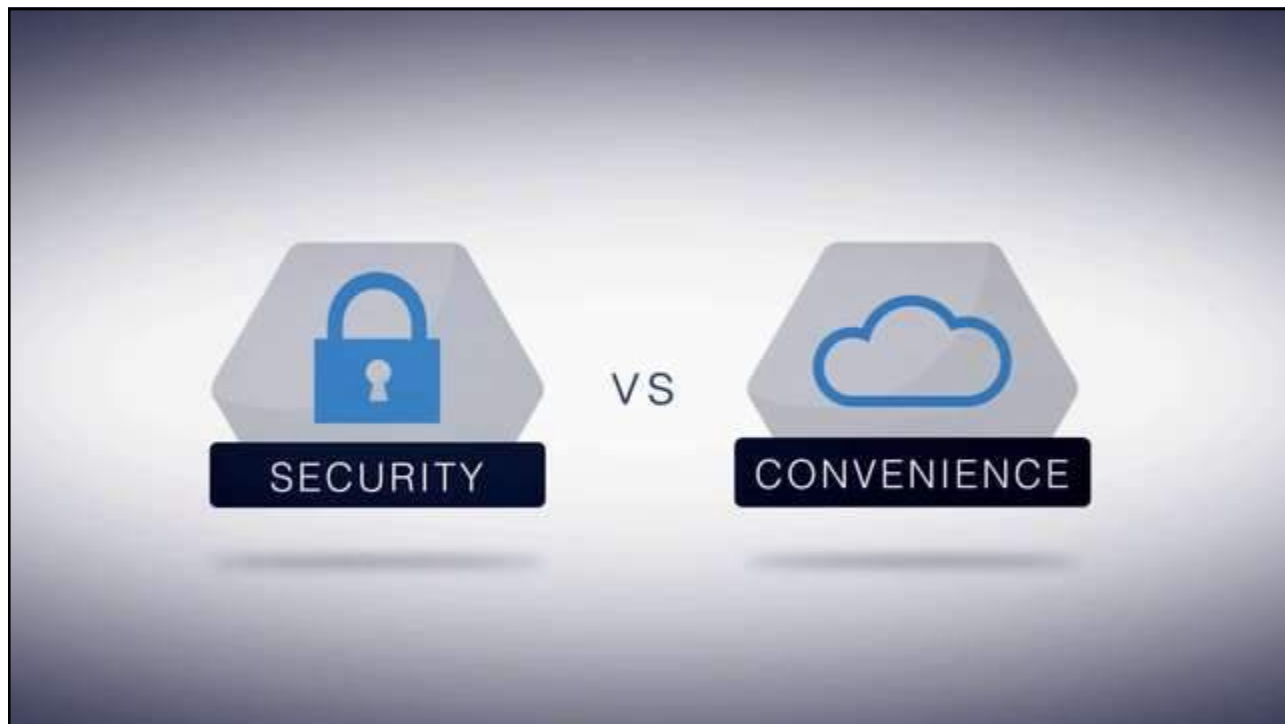   - New Adventures in Learning

Rob Truman
USN   Ret.

www.//geezertek.us
rob@geezertek.us

2

2

3

4

Malware

- Malware is one of the most common hazards to your computer when you're online, but it's easy to avoid.

- Developing safe and smart browsing habits can protect you from malware and other threats, like viruses.

- Securing your computer and learning how to identify and avoid suspicious links are the fundamentals of safe browsing habits.
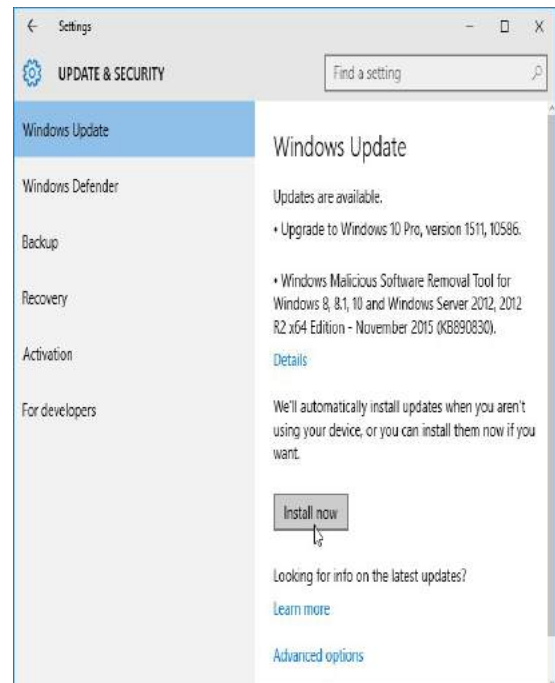
Rob Truman
USN   Ret.

www.//geezertek.us
rob@geezertek.us

5

Malware

- Malware & Viruses take advantage of security flaws in Windows and other software.

- **Keep your Operating System, Browser, and other Programs updated.**

- The security patches in these updates help make your computer immune to many threats.

Beware of Fake Pop-up Tech Support Scams

Security Warning

Suspicious Activity Found

During a routine scan, We've found a possible virus, we cannot automatically remove. Please call the number listed below to get step by step guidance to secure your computer.

Call Now:

+1-855-270-1376

We will guide you through the process to secure your computer step by step. In the meantime we strongly advise you not to use your computer for any sensitive processes like logging in or shopping online.

The Following Information Is At Risk:
- Credit card information
- Facebook chat history
- Login Information
- Webcam Images
- Skype Chat Information
- E-mail Login Information
- Bank Login Details

Do **not call the phone number** for support - it is not Microsoft's.

Rob Truman
USN   Ret.

www.//geezertek.us
rob@geezertek.us

This is a group of scammers waiting to rob you of hundreds of dollars under false pretenses.

7

PHISHING ALERT
SCAM-SPAM-MALWARE-SPYWARE

Phishing

8

Phishing

Phishing scams are messages that try to **trick you into providing sensitive information**.

These often appear to come from a bank or another trusted source, and they'll usually want you to re-enter a password, verify a birth date, or confirm a credit card number.
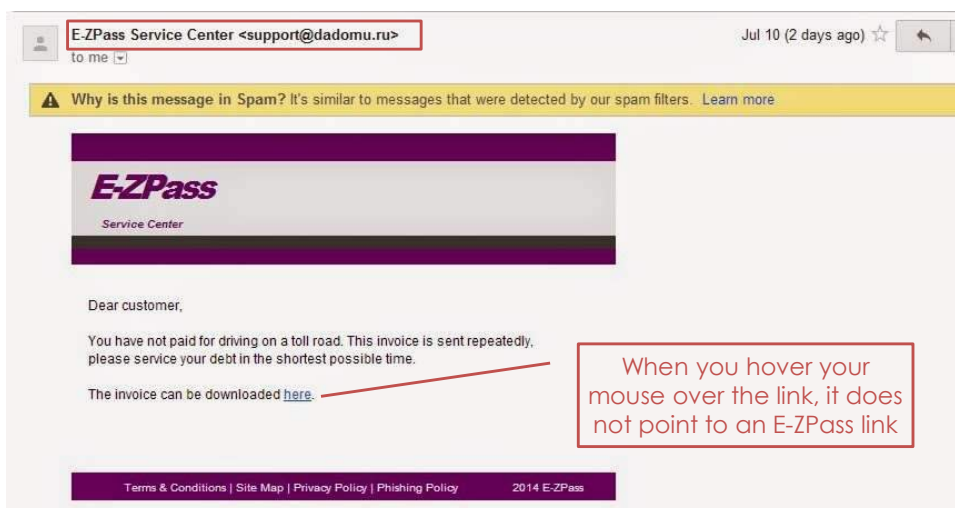

Rob Truman
USN   Ret.

www.//geezertek.us
rob@geezertek.us

9

Where Is It From?

E-ZPass Service Center <support@dadomu.ru>   Jul 10 (2 days ago)
to me

⚠ Why is this message in Spam? It's similar to messages that were detected by our spam filters. Learn more

E-ZPass
Service Center

Dear customer,

You have not paid for driving on a toll road. This invoice is sent repeatedly, please service your debt in the shortest possible time.

The invoice can be downloaded here.

When you hover your mouse over the link, it does not point to an E-ZPass link

Terms & Conditions | Site Map | Privacy Policy | Phishing Policy   2014 E-ZPass

Rob Truman
USN   Ret.

www.//geezertek.us
rob@geezertek.us

10

Where Is It From?

info@jmsc.co.**jp**	JAPAN
returns@amazon.com.**mx**	MEXICO
info@okinawatimes.com.**id**	INDONESIA
accounts@chase.**hu**	HUNGARY
returns@walmart.**cn**	CHINA
contact@your-bank.**de**	GERMANY
usa@amirl.co.**uk**	UNITED KINGDOM
admin@noseh.org.**ph**	PHILLIPINES
usa@smopy.org.**ru**	RUSSIA

Rob Truman
USN   Ret.

www.//geezertek.us
rob@geezertek.us

11

Phishing

From: "Bank of America" customerservice@bankofamercan.com
To: "Jane Smith" jane-smith12@gmail.com
Date: Wed, May 26, 2010

Subject: Fraud Alert – Action Required

Bank of America

Dear Customer,

At Bank of America, your satisfaction is our number one priority. We have recently added an Advanced Online Security option for our customers with online accounts. It is urgent that you go to our website and add Advanced Online Security to your account. Click on the following and update your information www.bankofamerica.com.

If you do not take these steps, in order to protect you, we will put a hold on your account, and you will be required to visit your local branch to verify your identity.

Thank you for helping us to make Bank of America the safest bank on the internet.

If you are receiving this message and you are not enrolled in online banking, sign up now. New online members will automatically be enrolled in the Advanced Online Security program.

Sincerely,

Bank of America Online Security Department

- Important Subject Lines

Rob Truman
USN   Ret.

www.//geezertek.us
rob@geezertek.us

12

6

Phishing

From: "Bank of America"
To: "Jane Smith" jane-smit
Date: Wed, May 26, 2010
Subject: Fraud Alert – Action Required

customerservice@bankofamerican.com

Bank of America

Dear Customer,

At Bank of America, your satisfaction is our number one priority. We have recently added an Advanced Online Security option for our customers with online accounts. It is urgent that you go to our website and add Advanced Online Security to your account. Click on the following and update your information www.bankofamerica.com.

If you do not take these steps, in order to protect you, we will put a hold on your account, and you will be required to visit your local branch to verify your identity.

Thank you for helping us to make Bank of America the safest bank on the internet.

If you are receiving this message and you are not enrolled in online banking, sign up now. New online members will automatically be enrolled in the Advanced Online Security program.

Sincerely,

Bank of America Online Security Department

Bankofamerica.com is
not the same as
Bankofamerican.com

Rob Truman
USN   Ret.

www.//geezertek.us
rob@geezertek.us

13

Phishing

From: "Bank of America" customerservice@bankofamerican.com
To: "Jane Smith" jane-smith12@gmail.com
Date: Wed, May 26, 2010
Subject: Fraud Alert – Action Req

Bank of America

Dear Customer,

At Bank of America, your satisf   have recently added an
Advanced Online Security option f   ounts. It is urgent that you go to
our website and add Advanced Online S   t. Click on the following and update
your information www.bankofamerica.com.

If you do not take these steps, in order to protect you, we will put a hold on your account, and you will be required to visit your local branch to verify your identity.

Thank you for helping us to make Bank of America the safest bank on the internet.

If you are receiving this message and you are not enrolled in online banking, sign up now. New online members will automatically be enrolled in the Advanced Online Security program.

Sincerely,

Bank of America Online Security Department

- It's easy to make a **copy** of any logo.

Rob Truman
USN   Ret.

www.//geezertek.us
rob@geezertek.us

14

7

Phishing

From: "Bank of America" customerservice@bankofamercan.com
To: "Jane Smith" jane-smith12@gmail.com
Date: Wed, May 26, 2010
Subject: Fraud Alert – Action Required

Bank of America

Dear Customer,

At Bank of America, your satisfaction is our number one priority. We have recently added an Advanced Online Security option for our customers with online accounts. It is urgent that you go to our website and a _____ e following and update your information **www.bankofamerica.com**

If you do not take these steps, in order to protect you, we will put a hold on your account, and you will be required to visit your local branch to verify your identity.

Thank you for helping us to make Bank of America the safest bank on the internet.

If you are receiving this message and you are not enrolled in online banking, sign up now. New online members will automatically be enrolled in the Advanced Online Security program.

Sincerely,

Bank of America Online Security Department

- Do not following links from this type of email.

Rob Truman
USN   Ret.

www.//geezertek.us
rob@geezertek.us

15

Exclusively for: | VALUED CUSTOMER
Online Banking

Bank of America

Your Bank of America accounts has been locked!

There are a number of invalid login attempts on your account. We had to believe that, there might be some security problems on your account. So we have decided to put an extra verification process to ensure your identity and your account security.

Please click here to continue the verification process and ensure your account security.

Email Preferences
This is a service email from Bank of America. Please note that you may receive service email in accordance with your

These "Account Issues" emails take the user to dummy login pages, where the hacker conveniently — and easily — grabs login credentials, and therefore bank account, credit card numbers, and more.

Rob Truman
USN   Ret.

www.//geezertek.us
rob@geezertek.us

16

Regards David Brown Cell: +15152032156 **VERY URGENT**

MR. DAVID BROWN **<k-abe@brown.plala.or.jp>** 4:24 AM (2 hours ago)

This message seems dangerous
Similar messages were used to steal people's personal information. Avoid clicking links, downloading attachments, or replying with personal information.

Looks safe

SCAM ALERT

This is David Brown from custom boarder protection homeland security Des Moines international airport Iowa USA, I write to know if you are ready now to receive your two military boxes which have been in this office for long time, the fee has been cut down to $350 usd, so kindly get back to me asap to enable me attend to you immediately and appoint one of our delivery agent to go ahead and complete your delivery to your location address you want the boxes to be deliver to you as soon as possible ok, Bear it in mind that this is last chance for you to receive your boxes okay.or it will be send to treasure department as an abandon shipment ok. Reply to me on this email below (officefile707@aol.com)

Rob Truman
USN   Ret.

www.//geezertek.us
rob@geezertek.us

MY FAVORITE!

17

Phishing Attacks

- 86% of Email Attacks Don't Involve Malware
- Apple Is the #1 Imitated Company in Phishing Scams
- COVID-19 Phishing Emails Are Booming

- Well-Informed Users Are the Best Defense Against Phishing Attacks.

Rob Truman
USN   Ret.

www.//geezertek.us
rob@geezertek.us

18

Ransomware

- Ransomware is a form of malware that threatens you with harm, usually by denying you access to your data.

- The attacker demands a ransom from the victim, promising — not always truthfully — to restore access to the data upon payment.

Rob Truman
USN   Ret.

www.//geezertek.us
rob@geezertek.us

19

Ransomware

4 Types of Ransomware

1. Drive-by Downloading
   - A user unknowingly visits an infected website and then malware is downloaded and installed without the user's knowledge.

Rob Truman
USN   Ret.

www.//geezertek.us
rob@geezertek.us

20

Ransomware

2. Scareware –
   - The simplest type of ransomware, aka scareware, consists of bogus antivirus or clean-up tools that claim they've detected umpteen issues, and demand that you pay in order to fix them.
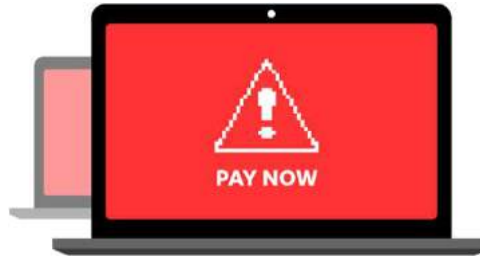
Rob Truman
USN   Ret.

www.//geezertek.us
rob@geezertek.us

21

Ransomware

3. Lock-Screen
   - These don't allow you to use your PC in any way.
   - They display a full-size window after Windows starts up— usually with an FBI or Department of Justice logo— saying that you violated the law and that you must pay a fine.

Rob Truman
USN   Ret.

www.//geezertek.us
rob@geezertek.us

22

Ransomware

4. I'm Screwed

- Encrypting malware such as Locky is the worst variant, because it encrypts and locks your personal files until you pay up.
- But even if you haven't backed up your files, you may have a chance to recover your data.

!!! IMPORTANT INFORMATION !!!!

"Locky" sets your wallpaper to make sure you know what to do next

Rob Truman
USN   Ret.

www.//geezertek.us
rob@geezertek.us

23

25

Strong Password

To protect yourself and your information, you'll want to use passwords that are:

- **Longer is better.**
- **Use special characters & numbers.**
- **Difficult for someone else to guess.**
- **Easy for you to remember**.

Weak Passwords	Strong Passwords
Password	\ne2o.P1/
12345678	&k1cO_282.lim)
JimBob	{Tr35uR3_hun2er/}
joedoe120171	

Rob Truman
USN   Ret.

www.//geezertek.us
rob@geezertek.us

26

Worst Passwords of 2020

1. 123456
2. 123456789
3. picture1
4. password
5. 12345678
6. 111111
7. 123123
8. 12345
9. 1234567890
10. senha
11. 1234567
12. qwerty
13. abc123
14. Million2
15. 000000
16. 1234
17. iloveyou
18. aaron431
19. password1
20. qqww1122

i shall use strong passwords.
i shall use strong passwords.
i shall use strong passwords.
i shall use strong passwords.
I 5ha!! u53 $4r0ng-p@5sw0rdz!

Strong passwords are a minimum of 8 characters in length & include uppercase, lowercase, numbers & special characters.
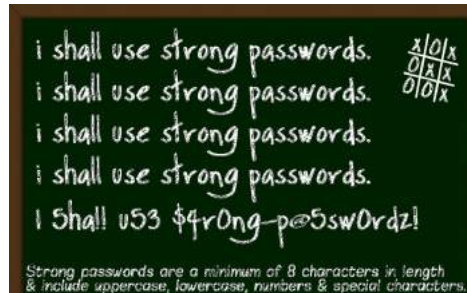
Rob Truman
USN   Ret.

www.//geezertek.us
rob@geezertek.us

27

Remembering Your Password

The Best Password Management Tools & Apps (Free + Paid)
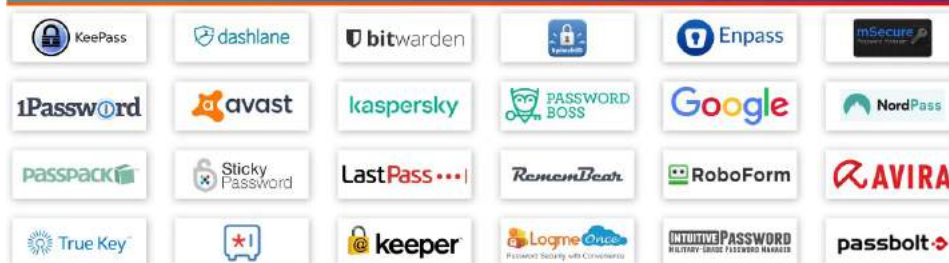
Rob Truman
USN   Ret.

www.//geezertek.us
rob@geezertek.us

28

What is a Passphrase

- The main use of a passphrase is so that a longer password than normal can be used and users can still remember it with ease.

- Oftentimes, a passphrase is used instead of a password manager to remember complex passwords and to avoid putting all of a user's passwords in one place.

Rob Truman
USN   Ret.

www.//geezertek.us
rob@geezertek.us

29

What is a Passphrase

- The time it would take a computer to crack a simple password such as "iphone" is .04 seconds.

- "iponemadebyapple" would take 15 days to crack.

- "iPhonemadeby@pple2" would take four years to crack.

Rob Truman
USN   Ret.

www.//geezertek.us
rob@geezertek.us

30

Random Password Generator

Cute Fun Brutal Price

Generate Another

Options:
Words: 4 | Remove spaces | Replace spaces with "-" | Add a number | Add a special character | Uppercase

https://randompassphrasegenerator.com/

Rob Truman
USN   Ret.

www.//geezertek.us
rob@geezertek.us

31

How secure is your Password

How secure is your password?

Tip: Don't simply change e's for 3's, a's for 4's etc. These are well-established password tricks which any hacker will be familiar with

Show password: ☑

Cute Fun Brutal Price

Very Strong

21 characters containing: ✓ Lower case   ✓ Upper case   ✗ Numbers   ✗ Symbols

Time to crack your password:
2 million years

Review: Fantastic, using that password makes you as secure as Fort Knox.

Your passwords are never stored. Even if they were, we have no idea who you are!

https://www.my1login.com/resources/password-strength-test/

Rob Truman
USN   Ret.

www.//geezertek.us
rob@geezertek.us

32

33

Secure Your Computer

Limiting your computer's vulnerability to malware is a crucial safe browsing habit.

You can protect your computer by running anti-virus & anti-malware software.

Even if you don't see signs of malware on your computer, running regular scans can catch any malware that has escaped notice.

Rob Truman
USN   Ret.

www.//geezertek.us
rob@geezertek.us

34

17

Top Rated Security Software

TOTAL AV

PC PROTECT

Bitdefender

McAfee

AVIRA

Norton by Symantec

avast!

AVG

Malwarebytes

SCAN GUARD

Rob Truman
USN   Ret.

www.//geezertek.us
rob@geezertek.us

35

What Software Should I Use?

What Is The Difference Between Anti-Virus & Internet Security Software?

Antivirus (AV) software provides a basic level of protection for your system. Internet Security expands on capabilities such as scanning files and software, activity monitoring and vulnerability search with features tailored for Internet use.

PAID VS **free**

Rob Truman
USN   Ret.

www.//geezertek.us
rob@geezertek.us

36

Antivirus, Deconstructed

- Four basic levels of antivirus products exist:
  - Free
  - Paid antivirus
  - Suites
  - Premium Suites.

- As you move up the ladder from free to premium suites, you typically pay more and get more features, such as identity theft protection, firewalls, parental controls, and system performance tools.
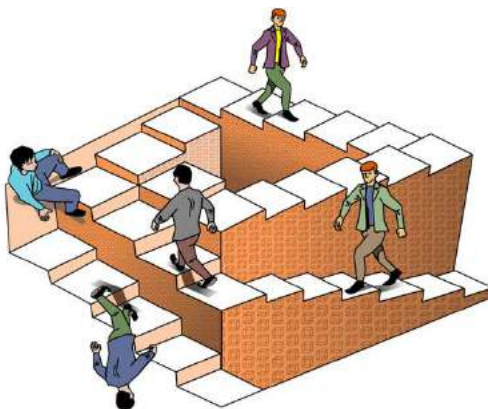
Rob Truman
USN   Ret.

www.//geezertek.us
rob@geezertek.us

37

38

Staying Safe – Browse Smart

- Always double-check the URL of your banking site, social networking site, and e-mail site before you log in.
- Type in the URL by hand, and to never follow links from an e-mail.
- Check for HTTPS instead of the less-secure HTTP.
- Most browsers, now include a color-change on the left side of the location bar to indicate that the site has been verified as legitimate.

Rob Truman
USN   Ret.

www.//geezertek.us
rob@geezertek.us

39

Email Tracking

The sender of the email embeds an invisible 1 x 1 pixel image, a so-called pixel tracker, into the message or an attached document.

When that email or attachment is opened, the email server requests that tiny image from the server where it's stored.

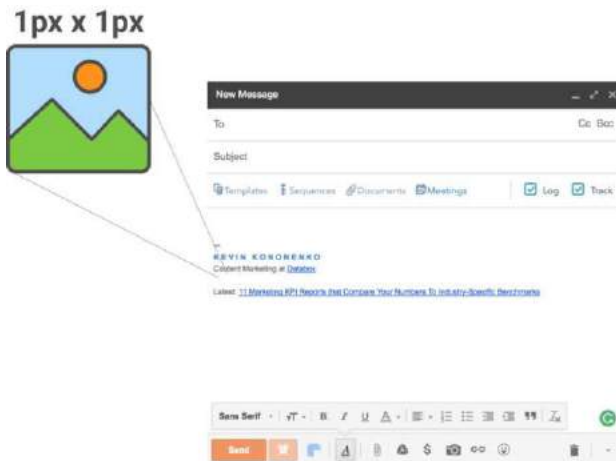That request betrays the opening time, the location, and the device, revealing your information to the sender

Rob Truman
USN   Ret.

www.//geezertek.us
rob@geezertek.us

40

Email Tracking

1px x 1px

Solution: Block your emails from automatically loading images.

Rob Truman
USN   Ret.

www.//geezertek.us
rob@geezertek.us

41

Browser Tips

- Delete cookies on close.
- Clear history on close.
- Webmail: Don't open images by default.
- Disable 'JavaScript'.
- Use HTTPS instead of HTTP sites.

Rob Truman
USN   Ret.

www.//geezertek.us
rob@geezertek.us

42

Browser Tips

- Enable 'Pop-up Blocking'.
- Turn-on 'Automatic Updates'.
- Enable 'Do Not Track'
- Use Incognito or Private Browsing for sensitive sites.

Rob Truman
USN   Ret.

www.//geezertek.us
rob@geezertek.us

43

Social Media Safety

- Use caution when you click links.
- Know what you've posted about yourself.
- Don't trust that a message really is from whom it says it's from.
- Type the address of your social networking site directly into your browser.

Rob Truman
USN   Ret.

www.//geezertek.us
rob@geezertek.us

44

Social Media Safety

- Do not allow social networking services to scan your e-mail address book.
- Everything you post to the Internet is permanent.
- Be careful about installing extras.
- Be selective about who you accept as a friends.

Rob Truman
USN   Ret.

www.//geezertek.us
rob@geezertek.us

45

Manage Your Privacy Settings

- Want to view or change your privacy/security settings, but don't know where to find them?
- **National CyberSecurity Alliance** provides a list of direct links to update your privacy settings to over 80 popular devices and online services.

- E-commerce
- Email/Voice Communication
- Food Delivery Services
- Mobile Location Services
- Music
- Photo & Video Sharing
- Search Enginges
- Web Browsers
- Social Networks

Rob Truman
USN   Ret.

www.//geezertek.us
rob@geezertek.us

https://staysafeonline.org/stay-safe-online/managing-your-privacy/manage-privacy-settings

46

Phone Scams

- **Give Them Nothing.** Your best defense is to tell them nothing.
- **Don't…**
  - Confirm your name.
  - Reply 'Yes' to any question.
  - Verify your address.
  - Do Surveys
- **Hang Up**

- **Other Tips**
  - IRS will not call you.
  - Microsoft is not monitoring your computer and will not call you offering to help.
  - Robocalls: Only say 'Hello' once or just hang up.
  - Never enter a star code in your phone.

Rob Truman
USN   Ret.

www.//geezertek.us
rob@geezertek.us

47

Rob Truman
USN   Ret.

www.//geezertek.us
rob@geezertek.us

48

https://geezertek.us

Rob Truman
USN   Ret.

www.//geezertek.us
rob@geezertek.us

49

50