Security Strategies 2018

More Important Every Day!

By

Rita Wronkiewicz

rwronk@gmail.com

Security

Q: What is the most important thing we should discuss tonight?

A: Anti-virus program latest rankings??

WRONG!!!

Maintaining Personal, Device and Network Security

- In 2018 it's MUCH more complex than installing a certain piece of software and assuming you're "covered"!
- Knowing and Following Appropriate User Behavior Is a Key Component in the Security "War"

SO Many Topics and Recommendations to Be Aware of!

- PC User Behavior
- Email and Spam
- Anti-virus and Anti-spyware Software
- Passwords
- Browsing
- Task Manager
- Deleting Old Accounts
- WiFi
- Backups

SO Many Topics and Recommendations to Be Aware of!

- Mobile devices
- Social Networking
- Phishing
- Installing New Software
- Data Encryption
- Deleting Old Accounts
- Recovering from a hack

PC User Behavior

- **Don't be your normal trusting self!**
  - **Remember that "social engineers" are highly skilled at manipulating you when they call or pop up or email you -- we are all attractive targets for hackers**
- **Don't respond to ads, emails, popups, phone calls that are "too good to be true" or "too scary to be real"**
- **Make device/PC security a priority, even if it takes more time/effort or more training – bring your questions to the forums or the computer lab sessions! We like to give advice!**

Email and Spam

- Share your email address only with people you know
- Sign in as a “Guest” or with no email address if you can when you buy something from a new website
- Create a second email account for websites that will send you Spam

Email and Spam

- Giving email address to sites can result in their selling it to other sites – multiplying # of Spam emails and increasing your chance of getting an email that infects your computer!

- The bad news:
  - SPAM is a byproduct of Internet use
  - You'll get some even if you're careful!

Email and Spam

- **Watch for pre-selected *checkboxes* on websites that allow them to send you junk mail or to sell your email address –> UNCHECK!**

- ***Ignore* messages that appear to come from Microsoft asking for your password or threatening to close your account –> FAKE!**

- **Don't DELETE Spam messages - Click the *Junk/Spam button* so that from now on they'll go directly to the Junk/Spam folder.**
  - **You want to "train" the filter to recognize what <u>you</u> consider Spammers.**

Email and Spam

- **Problem:** Win 10 Mail app has no spam filter. (You can move message to Junk folder, but no "training" occurs.)

- **Solution:** Go to your Webmail website occasionally and flag the spam messages there – they will get blocked at the server level and then won't appear in your Win 10 Mail app

Email and Spam

- **Unsubscribe from an emailing website when it makes sense:**
  - ***To do this => Click Unsubscribe button* at bottom of email (if there is one.)**
  - **If sending company is "legitimate", UNSUBSCRIBE**
    - **Sometimes there's a delay, so try again**
    - **If they don't stop, find a customer service email address or phone nbr on their website and contact them**
  - **If an "iffy" company, delete email and/or flag it as Spam**
    - **If you unsubscribe, you tell them you exist and you've verified that you're a valid email they can send to their nasty friends!**

Email and Spam

- If you get an email from a friend and it has an attachment or a web link, but no text that is personal in nature, DELETE it. It often resulted from your friend's email getting hacked.
- "You've Got to See This" or similar is almost always Spam with embedded viruses

Email and Spam

- **Pay attention to the wording, spelling and grammar in emails you get. Risky emails are usually written by people unfamiliar with our language and how we phrase things.**

- **"Special Offer for You", or similar, is almost always Spam with embedded viruses**

Email and Spam

REJECT IT!

(even if it's from someone you know)

- **If you didn't expect it**
- **If it says it's urgent and immediate action is necessary**
- **If you are told to click a link to prevent problems with your account**
- **Hint: If you can, contact your friend or the business by phone to verify if there is really an issue to resolve**

Email and Spam

- **NEVER include sensitive information like passwords, social security numbers, birthdates, account numbers in Email – EMAIL IS NEVER SECURE!**

(Just ask some of our Washington politicians…)

Anti-virus Software

- **Recommendation (My preferences, in order)**
  - Norton Security
  - Avast Free
  - Windows Defender (Win10 only)

  - This should be combined with
    Malwarebytes (anti-spyware program)
    - "Premium" is best, "Free" is okay if you can be diligent to run it weekly
    - Premium version has ability to schedule it to run daily without your intervention and has extra features like ransomware protection

Anti-virus Software

- **Other good source for anti-virus recommendations:**

PC Magazine link showing their latest reviews:
https://www.pcmag.com/article2/0,2817,2369749,00.asp

Anti-virus Software

- **My Anti-Malware strategy:**
  - **Set Norton Security to run FULL scan WEEKLY Schedule overnight**
    - **If you shut down every night, run during the day and click "run when idle"**
  - **Purchase 2-yr version of Malwarebytes for *all* your computers (good price per device!) and schedule it to run DAILY.**
    - **Click pull-down for additional schedule settings and tell it to quarantine, restart, etc. automatically.**
    - **Change setting to "Scan for Rootkits"**

Anti-virus Software

- **Need to examine settings on your anti-virus program to make sure the settings seem right and it's protecting you fully**

  E.g.., Trend Micro doesn't automatically quarantine "*Potentially Unwanted Programs*" – you need this!
  –> turn it on

  E.g.., Avast looks for virus definition *updates* every 4 hrs – this can impact your performance
  –> change it to 1440 minutes (DAILY)

Anti-virus Software

- In Windows 10, Windows Defender will start up automatically if it senses no other active anti-virus program
  - If you use it, watch for notifications in the Action Center about its status - and respond to them!

Anti-virus Software

- Always need to know if your anti-virus program is "happy"
  - If not, it's likely not protecting you well enough.
- Need to move the icon for your program down to the right side of the taskbar
  - Click the up caret (^) and find the *icon* for your anti-virus program
  - Drag it lower so it stays visible on the *taskbar*
  - Keep an eye on it →If it's not "happy", it'll likely have a red mark on it
    - If so, double click it and hit "Fix It" button

Password Protection

- Don’t use the same password for two accounts/websites!
- Longer is MUCH more secure
  - aim for 9 or 10 characters
- Include at least one of each of these:
  - numeric, capital, special character
- Remember that it’s not a PERSON who is guessing your password, it’s a fast computer!

Password Protection

- **Methodology that we like:**
  - Think of a sentence that is easy for you to memorize – like “I lived on Main Street in Los Altos”
  - Use the first letter of each word – **ilomsila**
  - If you like,
    - Change an “i” and/or an “L” to the number “1”
    - Change an “s” to a “$”
    - Capitalize the “la” to LA
    - Change “to” -> 2, “for” -> 4
      - **Possible result: 1lom$iLA**

Password Protection (cont'd)

- An extension of this:
  - Memorize the above result as your "base"
    - Don't memorize the characters, memorize the sentence!
  - Add two characters to this "base" each time you need a new password – so each password is unique but it's easier for you to remember
  - The two characters should be easy to remember
    - e.g., 1lom$iLAat for your AT&T account

Password Protection

Two-factor Authentication:

- I love it and I hate it!
- More secure than passwords alone

  (which aren't considered secure enough)
- It takes more effort because you have to provide at least one other "factor" to "prove you're you"

Password Protection

Two-factor Authentication

- You enter your password.
- You earlier provided the website or device with your cell phone number or landline number.
- They ask you to fill in more of the phone number than they're displaying

Password Protection

- If the number is accurate, they send you a text (SMS) or call you with a one-time number contained in the message.
- You enter this number and you've passed the test.
- Sometimes you can give them your pre-identified email address and they send the number via email.

Password Protection

- Even if it feels like an invasion of privacy, you need to provide backup email addresses and cell phone numbers to sites using this type of verification.
- To be really secure, you need to turn it on for sensitive sites even if it's not already on.

Password Protection

- If you can't verify with this second factor, you run the risk of getting locked out of important personal data – so make sure alternate email addresses and phone numbers are provided and up-to-date.
- This info is also used for "Forgot password" verification.

Password Protection

Why I "hate" it

- My cell phone is not handy or the battery is dead!
- A pickpocket stole my phone in the Paris train station last month, and all my sites pointed to the stolen cell phone number as my verification number!
- Some people don't have texting capability and some sites only accept texting you the code, not even a landline will work
- If you don't keep your "factors" up-to-date, it's a mess to get the website to let you in anyway

Password Protection

Why I "love" it

- Passwords alone have been proven to be insecure.
- It's better than getting hacked!

Password Protection

- Setting Up Security Questions:
  - Pick questions that are difficult for others to guess
  - Don't pick answer that is possibly on social media
  - BAD: what's the model of your first car? Not too many models to pick from, so easy for fast computer to guess.
  - Good Techniques:
    - Any question is okay – just give an answer that is irrelevant to the question -
    - Include numbers in the answer

BUT you must record/remember what you entered!

Password Protection

- **My favorite password assistant: ROBOFORM (or something similar)**
  - **You gradually build a website list**
  - **List is encrypted on your device and saved in the cloud so you can access it from all your devices**
  - **One *Master Password* allows you to access your password list**
    - **You enter it first time you open the browser and occasionally during the day when it asks again**

Password Protection

- To go to a website already in your list:
  - Hit "Roboform" (green robot) extension on your browser or phone
  - Pick a website from the list using the popup
  - Browser jumps to that website
  - Saved account & password for that site are automatically filled in
  - You're signed in and ready to go!

Password Protection

- To build a new entry in your list
  - Manually go to the site and enter in the account/password
  - Popup asks if you want to save that site in your list
  - If you hit “save”, an entry is created for that site with a recognizable name

Browsing

- Don’t let your browser save your account names and passwords on websites
  - (My exception) I let Chrome and Edge save my Gmail password so I can get right in
  - Use only current auto-updated browsers like *Chrome, Edge, Firefox, Opera*
- Use HTTPS sites where possible
  - they’re the only ones that are truly secure

Browsing

- Browsers get hacked too!
  - If you're getting unreliable responses or it won't start up, you need to do browser "reset" or uninstall & reinstall the browser
- Pay attention to the web address that appears when you link to a website (from your search result or from an email or web page link)
  - If it doesn't look like what you expected, click out of there FAST!

Browsing

- Always make sure you have at least two browsers installed – if one gets hacked, you can often still get to the internet with the other

- Do NOT use Internet Explorer in any OS – it's not considered safe enough technically

Browsing

- Clean out your “Search Engines” in your browser
  - Go to Settings and make sure Google, Bing, or your other favorite is default
  - Remove all others from the list
    - Especially “Ask”
- If your home page changes and you didn’t change it, you’ve likely been hacked
  - Change it back and then run Malwarebytes

Browsing

Use Adblock or Adblock Plus

- Go to Windows Store or Chrome store, etc. to install
- Keeps away malware type ads
- Has been downloaded on millions of PC's and Smartphones
- You can tell them to not block sites where you want to see the ads
- May be an issue as to who gets classified as approved (or not)

Browsing

- Review the “Extensions” installed in your browsers
  - If you don’t know what they are, they probably downloaded without your knowledge and can be considered malware

Task Manager

- Use your Task Manager to shut down Malware
  - To get to it, right-click any empty space on *Task Bar* and select "Task Manager"

- If you have app on your screen that you don't want and it won't go away:
  - Click its name on the Task Manager App list
  - Click "End Task" at bottom right to force it to stop right now
  - Sometimes it still won't stop ➔ reboot

Task Manager

- To make the bad app not start up every time you restart your computer
  - Click “More details” at bottom left of popup
  - Click “Startup” tab in Task manager and look for a similar name. If it’s there, Click it and then click “Disable”

WIFI

- For sensitive information (like shopping or banking)
  - Public wifi networks are a NO
- If you MUST access this type of info away from home -> use your cell phone
- Home routers CAN get hacked too
  ➔ reset was required last week for certain models due to malicious hack
- VPN's are recommended – Bob will discuss at Main meeting in near future

Phishing (i.e. “fishing”)

- Attempts to trick user into revealing personal/confidential info
- Can result in identity theft, stolen data to buy things, or any kind of fraud
- Usually done via email, but has spread to social media, messaging services and apps

Phishing

- **Email Phishing**
  - **Est. 135 million phishing emails sent each day**
- **Might be tricked to link to fake website**
  - **1.4 million *fake* websites created/month**

Phishing

- Some tactics used:
  - Bank looking to verify details
  - Online store attempting to verify non-existent purchases
  - "Tech support" analysist (says "Microsoft"!) claiming to be from a tech support company, needing access to your computer because he says it has been hacked and you're not safe
  - Answering "yes" to a phone question, they've then recorded your voice to answer questions for *illicit applications*

Phishing

- More tactics:
  - Attempts to panic the user
    – e.g., Urgent message from your bank
  - Feed on your greed – e.g. “You won a prize!”
  - Attempts to peak your curiosity – blank email with an interesting link or attachment
- Mass mailings – mostly ineffective, but they find enough uninformed people who just aren’t vigilant enough

Social Networking

- Social Media Phishing
  - Person “friends” whoever will let them, with fake picture and profile of him or her self.
  - Cons the person into sending them something using their fake persona
  - Communicates with them and inserts bad links (which may vary from a valid-looking web address by modifying it just a little so it looks real)

Social Networking

- **"Social engineering" is where attackers use whatever information they can glean from your public profiles – date of birth, education, interests – to try to get into your accounts on all sorts of services.**
- **People often use info on their social site as answers to security questions on passwords --- your pet's name or what school did you attend**

Social Networking

- Don’t post your whole life as “public”!
- Be careful who you friend – don’t “friend” anyone you don’t know or like
- Clean up your friends list
- Examine settings on Facebook etc. and add restrictions to limit your risk
- Don’t use real birthday, except on sites that require accuracy – but remember what you told them

Ransomware

- **Biggest problem on the Web!**
- **In 2016, over $1 BILLION stolen via *ransomware* – and last year grew by 748%!!!**
- **Techniques are "the usual"**
  - **Clicking on bad links in email or the web**
    - **Sometimes it works to just roll over a back link without clicking!**
  - **Opening infected attachments**
  - **Sending out millions of spam to see who they can catch**

Ransomware

- **What do they do?**
  - They hack into your system/device and effectively put your data into a box where you can see it but can't read, run, or update it
  - Whatever they encrypt is still there, but it is "encrypted" so it isn't readable without a "key"
  - They ask for money (usually *bitcoin*) to buy the key.
  - If you get the key, you can "decrypt" your files and your data is again accessible.
  - If you pay the money, MAYBE you'll get the key

Ransomware

- What makes them so dangerous
  - They're easy for criminals to implement – don't need to write complex software
  - *Bitcoin* payments usually make their actions untraceable
    - Some ransomware demands even include instructions on how to obtain the bitcoin to pay them off!
  - All it takes to infect a network is for one user to get fooled and launch a bad email attachment!

Ransomware

- Organizations pay the ransom because
  - they'll lose/disrupt their business if they don't get a quick fix
  - They don't choose to or can't afford the expense of securing data/systems/devices adequately
  - They don't want the public to know they weren't secured enough

Ransomware

- How do I protect my PC?
  - Install Antivirus/Antispyware software with Ransomware-protection capabilities
    - Premium version of Malwarebytes
    - Windows Defender (don't know how good)
  - https://www.nomoreransom.org
    - Portal containing growing number of decryption tools
      - Sponsored by McAfee, Kaspersky, Europol

Mobile Devices

- Lock your phone and possibly encrypt the data
  - Your phone can give access to your social accounts and more.
  - Once stolen, criminals can obtain email address, target your friends using your profile as bait, and even change your password.
  - Set your phone to time out at no more than a few minutes.

Mobile Devices

- Add an antivirus app (often free with PC anti-virus you buy)
- If your device gets stolen, change passwords for apps that are automatically tied to them
  - When my phone stolen, I changed my Amazon password!

Deleting Old Accounts

- Old unused accounts on websites may expose you to hacks in the future
  - First just try to log in and shut down the account on each old/unused site
  - Can refer to website "JustDeleteMe.com" for advice on more difficult deletions

Deleting Old Accounts

- e.g., Microsoft and Yahoo – if you delete your account, anyone can register for your email address after a grace period. What if that site is still connected to YOUR credit card or personal info?
- May have to contact their customer service

Backup Backup Backup

- **Use Win 10 File History or Win 7 Backup**

  AND

- **Use One Drive or Google Drive or other Cloud service**

- **Check your backup occasionally, at least to see if there is new data there**

- **Need regularly scheduled offline backup to guard against Malicious Encryption**