Security Resources

January 13, 2020

Viruses and Malware

Use a good antivirus program. The built in Windows Security was recently named as the top antivirus. You don't need a paid antivirus.

Keep your antivirus current. Generally it will update automatically, but if you get a warning notice be sure to update. If you are using a paid antivirus product make sure your subscription hasn't expired. An expired program will continue to protect you, but only from viruses it knows of from before your subscription expired.

Use Malwarebytes. The free version is good, but you must remember to run it periodically. If you want continuous protection get the paid version. Malwarebytes does not interfere with your antivirus and protects against malware, more common today than viruses.

Hacking

Keep your Windows patched.

Keep all software patched.

Keep your hardware patched.

When you get notifications that software or hardware needs to be patched, do it immediately. Yes, you are busy doing something else right now, but it is **important**! Updates sometimes add new features but the majority of them are for security reasons. If you are unpatched you are at risk within hours of a patch being released as hackers reverse engineer the patch to see the vulnerabilities it fixes. Don't let them be faster than you.

Check your windows updates in the Settings under Update and Security.

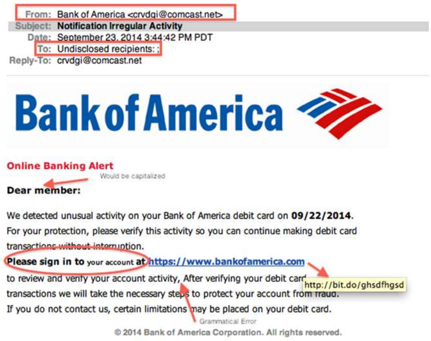
The worst attacks of 2019 https://www.zdnet.com/article/the-scariest-hacks-and-vulnerabilities-of-2019/?ftag=TRE-03-10aaa6b&bhid=93351105

Phishing and E-mail

Be careful with e-mail. Check to see who it is really from and where that link is taking you by hovering your mouse pointer over the return address and link. Be cautious because a link can look almost like the real thing such as www.bankofamerica.xyz.com.

If you get an unexpected e-mail from a company you do business with asking you to log in use a dummy password and see if it accepts it. If it does, it isn't really them and you haven't given your real password. Better yet, never use a link from an e-mail, go to the site from your browser.

Look for warning signs:



From: Bank of America <crvdgi@comcast.net>
Subject: **Notification Irregular Activity**
Date: September 23, 2014 3:44:42 PM PDT
To: Undisclosed recipients: ;
Reply-To: crvdgi@comcast.net

Bank of America

Online Banking Alert

Dear member:

We detected unusual activity on your Bank of America debit card on **09/22/2014**. For your protection, please verify this activity so you can continue making debit card transactions without interruption.
Please sign in to your account **at** https://www.bankofamerica.com to review and verify your account activity, After verifying your debit card transactions we will take the necessary steps to protect your account from fraud.
If you do not contact us, certain limitations may be placed on your debit card.

© 2014 Bank of America Corporation. All rights reserved.

Don’t open attachments from e-mail until you are certain it is legitimate. Attachments can be used to give hackers access to your computer. Frequently they will say you owe money and the invoice is attached or you have a FedEx or other delivery package that was undeliverable.
Don’t try to unsubscribe from spam e-mails, just block them and report as spam. Trying to unsubscribe simply tells the spammer that your address is good and can be sold to other spammers.
Ransomware. Have a backup so that if you are hit you can get your data back. Never pay ransom. Contact someone to come and clean your computer and restore your data.

Browsing the Internet
Make sure sites are HTTPS not HTTP if you are going to share any information.
Always log out of a site that you have logged on to at the end of the session.
When setting up an account that asks for personal information, lie. Use a made-up birthday or pets name or other security question and make a record of it in your password manager in case you need it again later.
Check your security settings for your browser.
In Chrome
https://support.google.com/chrome/answer/114836?co=GENIE.Platform%3DDesktop&hl=en
In Firefox https://www.wikihow.com/Change-Your-Security-Settings-on-Firefox
Brave https://support.brave.com/hc/en-us/articles/360017989132-How-do-I-change-my-Privacy-Settings- which also includes security settings.
There is a new version of Microsoft Edge coming, so it is unclear at this time how to adjust the security settings.
When joining a new site watch for pre-checked boxes offering to send you e-mails or otherwise annoy you.

Scams
Be aware of scams that are going around. AARP is a good source.
https://www.aarp.org/money/scams-fraud/
Some Current Scams:
IRS calling or e-mailing about unpaid taxes.
Social Security will suspend your account.
The IRS and Social Security will not call or e-mail you, they will send you a letter.
Grandchild in trouble or jail. Attorney will fix, just send money for bail or fine.
PGE will shut off your power.

Remember, no real business or government entity will call you demanding instant payment, and they don't take gift cards.

Go to jail for failure to appear for Jury Duty.

"Microsoft" calls and says something is wrong with your computer. Microsoft will never call you.

Virus Alert splash page telling you to call a number to get it taken care of.

Don't let anyone remotely log in to your computer unless you know who they are and trust them.

1 ring calls. Never call back an unknown number that rings just once. Don't return calls from these area codes, the rate can exceed $20 for the first minute:

268, 284, 473, 664, 649, 767, 809, 829 and 876.

Don't send money to someone you meet online. Scammers use dating services to meet you and then ask for money to travel to meet you in person.

Be sure that charitable requests are indeed a legitimate charity. When in doubt, look them up online.

An email claiming they have proof that you have been on porn sites and they will expose you.

Identity Theft

Protect your information.

If you are a victim of identity theft, submit a report about the theft to the Federal Trade Commission's website or call the FTC's toll-free hotline at 1-877-IDTHEFT (438-4338). You can also file a report with the local police department although they are sometimes less equipped to handle these complaints.

Don't carry your Social Security Card.

Don't give people your Social Security number when it isn't needed, such as doctors.

Your Social Security card is not to be used for identification except for things involving your credit and your social security. Too many businesses and organizations ask for it unnecessarily.

Check your Credit reports.

You may obtain a free annual copy of your credit report from each of the three credit reporting agencies by visiting www.annualcreditreport.com or by calling 1-877-322-8228. You can request information regarding fraud alerts, security freezes, and identity theft from the following credit reporting agencies:

- Experian, https://www.experian.com/help, 1-888-397-3742, P.O. Box 9554, Allen, TX 75013
- TransUnion, https://www.transunion.com/credit-help, 1-888-909-8872, P.O. Box 2000, Chester, PA 19016-2000
- Equifax, https://www.equifax.com/personal/credit-report-services, 1-800-685-1111, P.O. Box 105788, Atlanta, GA 30348

You may also get a free copy of your credit report at any time if you are turned down for credit.

Be cautious of offers for "free credit reports". The first one is free, but they try to sign you up for an annual service to "protect your credit." If they ask for a credit card cancel the transaction.

Many credit card companies also offer free credit scores. These are only your credit score, not your credit report. While useful, it won't make you aware of any inaccurate information in your credit report that may damage your credit score.

Put a freeze or alert on your credit report. This prevents anyone from taking out credit in your name. There is no longer a charge for this service. You can then do a temporary unfreeze if you are applying for credit.

Tax fraud can occur when someone applies for your refund before you do. Try to do your taxes as early as possible to decrease the risk. If you are the victim of Tax ID theft, you can contact the IRS.

Credit Card fraud can occur anytime someone has access to your credit card information. To lessen the risk don't store your credit card information on websites you buy from. Although there is little you can do, be aware that when you give someone your credit card, such as at a restaurant, it is possible for them to copy the information and use it or sell it.

Watch for "skimmers" on ATM machines and at gas stations. A skimmer mounts over the regular card reader and copies your information when you insert the card and sends it to the thieves.

Don't use standalone ATM machines such as are found in convenience stores and airports. Thieves have been known to install these boxes and actually give you money while stealing your credit card information for later fraud.

Always use a chip credit card, not a swipe. The chip creates a transaction with a dummy card number which can't be reused if stolen. A swipe records your actual account number. Phones with "digital wallets" such as Apple Pay and Google Pay also use a dummy number.

Try not to use your bank debit card. Credit cards provide protection against misuse of your account, limiting your loss to $50. Usually they will not charge even that unless you wait too long to report it. Debit cards have no recourse to the place where the theft took place so, generally speaking, your money is gone for good. Most banks will try to help but there is no guarantee they will be successful.

Put an alert on your credit card for transactions over a certain amount. The company will contact you whenever there is a higher transaction. Set the number above your normal amounts so you aren't being constantly bombarded by notifications. This will give you a heads up whenever an unusually large transaction occurs.

Dispose of unwanted or expired credit cards properly. Be sure to cut through the numbers and the chip or shred. Don't put the whole card in the trash at once, spread it over different trash pickups.

Be careful with your checks. Your check includes the bank's routing number and your account number. With a little more information these can be used to loot your account.

E-commerce fraud occurs when an unscrupulous company sells you something over the internet or by phone. Results can be you never receive the product, the product isn't what was promised, they use your credit card number to bill you for other things or they sell your credit card information. When dealing with an unknown vendor check with your bank to see if you can get a one-time credit card number. If the number is stolen it won't be any good.

Check your credit card and bank statements when they come for anything you don't recognize. Banks will correct any errors if you notify them within a limited time. Remember that it may take several weeks before your money is restored.

Medical ID theft.

This occurs when someone gets your health insurance information and bills on your policy.
If you are the victim of medical ID theft, notify your insurer and Medicare, get copies of your medical files and ask to have them corrected. You can also consider filing a health-privacy complaint with the U.S. Department of Health & Human Services online or call 1-800-368-1019. Be sure to check your Medicare records when they arrive. If anything looks questionable check on it. Be aware that not every unknown charge is fraud. There may be charges from doctors you have never seen because they have read MRI's or X-rays or done other diagnostic work.

Passwords

Don't re-use passwords.
Don't write your passwords down and store in an easy to find place (like taped to your monitor).
Don't share your passwords with anyone you don't completely trust.
Use a Password Manager!!! Go to http://donna.members.sonic.net/Password%20Managers-10-14-19.pdf for the presentation on password managers.
Best Practices:
Let the password manager create complex passwords. Don't worry if you can't remember them, that's the password managers job.
Don't let the password manager autofill on important sites such as banks and brokerage accounts, especially on a laptop.
Don't use common words. If you do, change capitalization and letters e.g. paSsw0rD. Common words are easy to hack with what is called a dictionary hack.
Don't use your birthday, pet's name or any other personal thing that can be easily discovered.
Use pass phrases with 20+ characters if you want a password (passphrase) you can remember such as mYfavoritegrandchildisbillY.
For important sites use 2 factor authentication. This means that when you try to log on with your password you will be required to provide additional proof that it is you. This can be a text message sent to your phone, a phone call, an e-mail or a physical device such as the Yubico Yubikey 5 NFC or Google Nest Tag. The physical devices will authenticate you just by being near your computer or phone.
Use Biometric authentication, usually a fingerprint or facial scan.
Have your passwords been compromised? Have you been pwned (owned in leetspeak)? Go to https://haveibeenpwned.com/ to enter your e-mail to see if it is part of a data breach. Google Chrome now has an extension to check your passwords to see if they have been compromised. It will also work with Brave and should work with the new Microsoft Edge coming out in January 2020. It is available at https://chrome.google.com/webstore/detail/password-checkup-extensio/pncabnpcffmalkkjpajodfhijclecjno
Firefox also has a tool at https://monitor.firefox.com/ to see if your email address has been compromised.
Per Wikipedia It is estimated that in first half of 2018 alone, about 4.5 billion records were exposed as a result of data breaches.

Wi-Fi

Make sure your home Wi-Fi is using WPA2 Personal encryption, not WEP.

Make sure your router is kept up to date to prevent hacking. Generally, a Comcast or ATT router will update itself automatically.

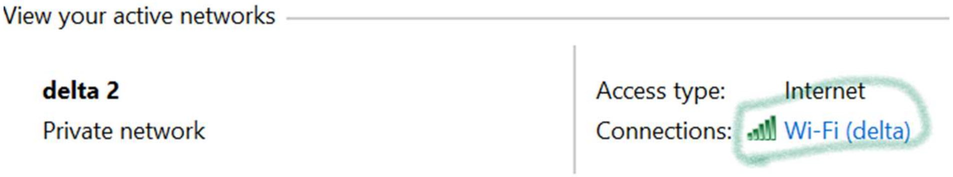
When you are using a public Wi-Fi network, such as Starbucks or a hotel, use a VPN (Virtual Private Network). If you are a Sonic customer, they have a free VPN app called Open VPN Connect. You can find info on the Sonic website. Otherwise, do a Google search for VPN and look for ratings and then select one. There will be an annual fee but it will potentially save you money and grief.

Never do anything like banking, using your credit card or any other sensitive transaction on hotspots without using a VPN. Just because the hotel or coffee shop requires a password doesn't mean it is safe.

When you log into a new network you will be asked if you want to be visible on the network. If it is **not** your own network, select public.

Change your router password. Depending on who supplied your router and the model it may not be necessary or possible to change the password. If the listed password is a unique combination of letters and numbers, you do not need to change it. If you do change it be sure to store it in your password manager because the information on the router will no longer be correct.

To change your password log on to your router and in the settings change your default password. To find your router address open Settings and go to Network and Internet. Click on Network and Sharing Center. In the active network section select your network and click it.

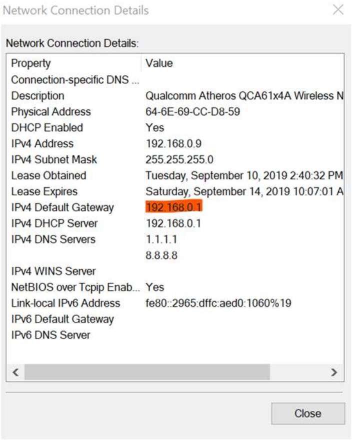


View your active networks

delta 2
Private network

Access type:	Internet
Connections:	Wi-Fi (delta)

In the box which appears click on details. The IPV4 Default gateway is the address of your router.



Network Connection Details

Network Connection Details:

Property	Value
Connection-specific DNS ...	
Description	Qualcomm Atheros QCA61x4A Wireless N
Physical Address	64-6E-69-CC-D8-59
DHCP Enabled	Yes
IPv4 Address	192.168.0.9
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	Tuesday, September 10, 2019 2:40:32 PM
Lease Expires	Saturday, September 14, 2019 10:07:01 A
IPv4 Default Gateway	192.168.0.1
IPv4 DHCP Server	192.168.0.1
IPv4 DNS Servers	1.1.1.1 8.8.8.8
IPv4 WINS Server	
NetBIOS over Tcpip Enab...	Yes
Link-local IPv6 Address	fe80::2965:dffc:aed0:1060%19
IPv6 Default Gateway	
IPv6 DNS Server	

Now that you have the number enter it in your browser with no http or www just something like 192.168.1.1. This will take you to the router sign in screen. The default router password will

usually be on a tag on the router. Depending on your router model you will have to hunt around for the password reset screen. Change the password and save.
How to secure your router https://www.wired.com/story/secure-your-wi-fi-router/
While you are in there check to see if there is a firmware upgrade available. If so, install it following the onscreen instructions.
To check what type of security your wi-fi has follow the instructions above to enter your router and go to the wi-fi section. Here you can check what kind of security you have and, depending on your ISP and router, you may be able to change the password as well.

Traveling

If you think that you may need a charge at the airport or on a plane, use your own charger plugged into an outlet or carry a portable charger. A public USB plug is not secure. You can buy a device such as a Portapow USB Data Blocker for use with public charging stations. This provides a layer of security between your device and the outlet.
At airports and hotels be careful. Criminals will set up their own Wi-Fi hotspots with similar names to trick you. Ask the hotel for the exact name of their Wi-Fi hotspot.
See above for safe use of public wifi.

Protect Your Data

Be sure to remove your data from old devices before disposing of them.
How to securely erase the data off your iPhone or iPad, Android device, Windows PC, hard drives, SSDs, and flash drives https://www.zdnet.com/article/how-to-securely-erase-the-data-off-your-iphone-or-ipad-android-device-windows-pc-hard-drives-ssds-and-flash-drives/
Always have a backup. Ideally you should have a local backup using an external hard drive, not a USB memory stick. In Windows go to Settings/Update and Security. In the backup section turn on File History and direct it to your external drive. Additionally, you may want to use a cloud backup. Remember the evacuation and fires? If all your files and photos are in the cloud that is one less thing to worry about. There are many free services available depending on the quantity of data you want to back up. Bonus: If you are away from your computer and need something from your files, you can log on to any computer and retrieve the data just by logging in to the cloud website.
If you are truly paranoid you might consider using encryption for your hard drive. If you are running Windows Professional, it is already built in. If not, you can install an encryption app. Just don’t lose the password or your data will be gone forever.

Protect Your Phone

Lock your home screen – Face recognition, fingerprint, password, pattern or pin.
Check your security settings. Do a search for your phone models security setting to see how.
Get an antivirus app if not included. The most recent phones are fairly well protected but if your phone is more than 3 years old consider an antivirus such as the free Lookout app for Android phones. There is also a free phone version of Malwarebytes.
Check your App permissions. Many apps request far more access to your phone than necessary, such as a flashlight app wanting access to your contacts and location. Be sure when installing a new app to be aware of what permissions it is requesting.

Be careful when installing apps. While Apple and Google do their best, sometimes a bad app makes its way onto the store. Stick with apps with lots of downloads and high ratings and you should be okay. Don't install apps from outside the Apple or Google stores.
When using public Wi-Fi follow the same rules as for a computer.
If you need to do sensitive internet from your phone when you are not on your own network and don't have a VPN, turn off wi-fi and use your phones data network which is secure. Don't forget to turn wi-fi back on when you are done to prevent excess data fees.
Make sure to install updates and patches. On Android the free app Snoop Snitch will check to see if your phone is up to date. Set your phone to automatically update installed apps.
Beware SIM Swapping. Sim swapping occurs when someone gets access to your phone account information and uses it to get a phone sim card on your account. That gives them access to all of the information on your phone.
Keep an eye on your device. Phone theft is rampant. Setting it down on the restaurant table while you go to the restroom is an invitation to have it stolen. When using your phone in public be aware of your surroundings to decrease the chance of someone grabbing your phone out of your hand. If you keep your phone in a purse, make sure it can't be grabbed by a passerby. Either bury it or keep your purse zipped.
I Phone users can check here for more security tips https://www.zdnet.com/article/how-to-keep-hackers-snoopers-and-thieves-out-of-your-iphone/?ftag=TREc64629f&bhid=93351105

Mail and Package Theft
Report mail theft to your local Post Office.
Post Office Informed Delivery will e-mail you with what mail is due to arrive. Get it at www.informeddelivery.usps.com This will help you to determine if something is missing.
Take your outgoing mail to the Post Office, don't leave it in your mailbox with the flag up.
Consider getting a Post Office Box or locked mailbox.
If you get Amazon deliveries, you can have them sent to an Amazon Locker location where you can pick it up. Local locations are GNC in Windsor, Whole Foods in Coddingtown and Rite Aid in Healdsburg. Do this if you have anything expensive coming.
Security cameras and doorbell cameras can give you added protection, making it possible for police to identify a suspect if something is stolen from your porch or your home is burgled.
Get sensitive documents online. Have bills, credit card and bank statements, W-4's and brokerage statements sent to you by email or retrieve them from their websites.

Protect Your Home
Get an alarm system (AARP members get 15% off at Simpli Safe). Either a monitored system or cameras and sensors can work, some with no monthly fee. If you have an Alexa device, it can be programmed to recognize the sound of breaking glass and alert you.
Install Security cameras.
Install smoke and carbon monoxide sensors and check the batteries twice a year. When daylight savings begins and ends is a good time to remember to do it. New "smart alarms" can even notify you if you are not at home.
Make sure your insurance coverage is up to date. Too many people learned after the Tubbs fire that their outdated insurance would not come anywhere close to replacing their burned homes.