HOW TO SECURE YOUR LIFE

Table of Contents

HOW TO REINSTALL WINDOWS 10

1. **BACKUP all your files and passwords!**
2. **NO, really! Everything will be deleted! Everything!**
3. Type "reset" into the Windows search bar
4. Click "reset this PC"
    a. Follow prompts to reinstall Windows
    b. Cloud install
    c. Keep nothing
    d. This will take some time, it will download everything needed to refresh your PC and install them
5. Once installed connect to internet
6. Type "update" in the Windows search bar
7. Install updates (will take several reboots and quite a long time)

HOW TO SECURE WINDOWS 10

1. Open browser and go to https://brave.com/download/
    a. Download and install Brave
2. Go to https://www.bitdefender.com/solutions/free.html
    a. Download Bitdefender Free and install
3. ALWAYS USE A VPN (Virtual Private Network) if you can!
    a. Only disconnect from your VPN if you run into a problem, and hop back on as soon as you can
    b. Install your VPN and sign in
    c. Configure VPN kill switch to be enabled
4. In Brave, install BitWarden https://chrome.google.com/webstore/detail/bitwarden-free-password-m/nngceckbapebfimnlniiiahkandclblb
    a. Sign up for BitWarden
    b. Use a Secure Master Password
    c. Use Two Factor Authentication (2FA, below at 12)
    d. Log in to BitWarden
5. Log into EVERY ONE of your accounts and
6. Change password to a unique randomly generated password generated in BitWarden
7. Save the login in BitWarden
8. Enable 2FA (Two Factor Authentication)
    a. Install Google Authenticator app on phone from the normal app store
    b. Log into the website to enable 2FA on and go to 2FA settings
    c. Scan the QR code in Google Authenticator app or Authy app
    d. Follow directions

   e. **Save the backup codes in Personal Vault in One Drive!**
      i. Open personal vault in One Drive
      ii. Type "OneDrive" into Windows search bar
      iii. Double click personal vault
      iv. Follow instructions to log in
   f. Save backup code to this personal vault
9. Set up Windows Hello
10. Type "hello" into Windows search bar
11. Set up face login
12. Set a SECURE pin for login not used elsewhere and not shared with anyone
13. Install all your applications you usually use FROM THE OFFICIAL SITE (Google for it)
14. Restore any files and backups you have
15. If restoring from a removable drive SCAN THE DRIVE WITH FORTICLIENT before transferring any files
16. Ensure device encryption is on
   a. Type "encryption" into the Windows search bar
   b. Open "device encryption settings"
   c. Ensure its on. In the event encryption is off, turn it on

ROUTINE SECURITY

1. Make sure anti malware (Bitdefender Free) is scanning and updating routinely
2. Always install updates for every piece of software when notified to do so
3. DO NOT CLICK ANY LINK IN ANY EMAIL/TEXT/DM/ETC
   a. For example, if the email is from Netflix with a notification, log into netflix.com in a separate tab and not follow the link in the email
   b. If the email is to track a package, copy and paste the tracking number into the proper website (usps.com, ups.com, netflix.com, etc.)
4. DO NOT DOWNLOAD AND INSTALL ANYTHING FROM A NON-TRUSTED SOURCE
   a. If an application needs to update for any reason, go to that applications website (Google for it) and download the program from there
   b. Fake update messages are common on the internet
5. DO NOT INSTALL BROWSER EXTENSIONS FROM OUTSIDE THE BROWSERS EXTENSION STORE
6. KEEP MULTIPLE BACKUPS
   a. At least two in the cloud (one drive, drop box, google drive, etc.)
   b. At least two on physical hardware or external hard drives
      i. One should be a full Windows weekly backup
   c. Type "backup" into the Windows search bar
   d. Open "backup settings"
   e. Set up "backup using file history"
   f. Set this to your external hard drive

            i. The other should be a backup of your critical files and settings separately, done manually by copy and pasting important files to an external drive that is disconnected unless being used for backups.

7. Ensure all applications and Windows update automatically
8. Reboot your computer at minimum once per day
9. ALWAYS lock your computer when stepping away, even for a minute. the keyboard shortcut for this [Windows logo key] + L at the same time
10. Beware any phone call, email, text, IM, etc. telling you that you have a virus, they will try and get you to download something or give them access to your computer. THIS IS ALWAYS A SCAM
11. PASSWORDS ARE LEAKED ALL THE TIME
    a. Always use a new, different, randomly generated password for EVERY SITE
    b. A common scam is to get an email or phone call with a leaked password of yours, claiming to have compromising video of you or something. THIS IS A SCAM! Delete and ignore.
    c. Use 2FA (2 Factor Authentication, described earlier) on ALL websites that support it!
        i. Use the **Google Authenticator** app or **Authy app** and NOT text/SMS messages wherever supported!
12. Text/SMS messages are not nearly as secure as the authenticator app, but much, much better than nothing!
13. Verify all login pages start with **https://** and NOT http://
    a. **https://** means the connection is encrypted and http:// is not encrypted, so never send passwords or payment details over any address starting with http://

EMAIL AND ACCOUNT SECURITY

1. It is very important to use multiple email addresses
    a. One should be your “spam address” any email address required to sign up for anything “low security”
    b. Another for business or personal use
    c. One last one for financial, banking, cryptocurrency, etc. “high security” applications, do not share this one and only use it on the “high security” accounts

SCAMS

1. Advertisements on social media are often scams! Not always but be careful! No matter how good a product looks, proceed with great caution, and google to see if the retailer and product are reputable.
2. Anyone trying to blackmail you online is lying. Don’t pay out!
3. Read about common scams and stay on top of them!
4. VERIFY ALL LOGIN PAGES BEFORE LOGGING IN! No matter how legitimate they look, verify that the website address is 100% correct and accurate.
    a. The DOMAIN is what you need to verify. the format of a domain is subdomain.**domain.com**/specificpage So ensure, for example, if you are logging into google,

that it looks something like IgnoreThis.**GOOGLE.COM**/IgnoreThisToo or for amazon, it looks like IgnoreThis.**AMAZON.COM**/IgnoreThisToo.

b. Always navigate to the login page normally or from google, NOT from a link sent to you in any way! These links can look very legitimate and can even be faked or compromised in some cases!

c. DO. THIS. EVERY. SINGLE. TIME.

5. If you receive a security warning from your browser or your antimalware, DO NOT IGNORE IT. Stop what you are doing and try again later.

   a. Often security warnings on web pages can be caused by a simple error on the end of the website.

   b. This does not mean you should ignore it!

6. NO GOVERNMENT OR LEGITIMATE AGENCY WILL DEMAND ANY PAYMENT WITH BITCOIN OR GIFT CARDS

   a. Anyone demanding any payment in bitcoin, cash, money order or gift cards unexpectedly is a SCAMMER

   b. The IRS OR ANY OTHER AGENCY WILL NEVER CONTACT YOU FOR IMMEDIATE PAYMENT or you will "get arrested" THIS IS A SCAM

   c. Anyone who wants to stay on the phone with you while collecting an unexpected payment IS A SCAMMER

   d. ANYONE requesting an unexpected payment, or even an expected payment in an usual, unexpected way is A SCAMMER

   e. Scammers will always give you a great sense of urgency and will routinely threaten you! Examples being

7. Pay NOW or get arrested

   a. Pay NOW or we will release your sex tape (often included with a leaked password they can google for)

   b. Pay NOW or we will delete your files

   c. Pay NOW or we will kill you

   d. Pay/call/IM NOW because you have a "virus"

      i. Often will try to connect to your computer

      ii. Are often associated with fake web pages showing a "virus alert" or similar

      iii. These fake alerts can be very convincing. Rely on Microsoft Security (Windows built in antivirus) and FortiClient, and nothing suggested over the phone/email

8. Learn to spot suspicious links

   a. they are often like, but not exactly like legitimate websites.

   b. examine the DOMAIN carefully

9. The format of a web address is: subdomain.**DOMAIN.COM**/webpage

      i. Ensure the DOMAIN is correct

        ii. Do not click any link from someone you do not know! No matter how legitimate it looks, log into the website as you normally would NOT by the link and check for a notification.
    b. scammers often use URL shortener like bit.ly, be suspicious of these links! URL shorteners have legitimate use, but the source is the key: if you do not trust the source, DO NOT CLICK THE LINK

10. Always use your VPN unless you run into a problem, then only leave it disconnected as short a time as possible
11. Unless there is a clear reason to do so, with a trusted service, do not scan or take pictures of your ID or any other documents
12. Never share any private information at all unless there is a clear reason and it's a trusted service requesting it
13. Do not plug in randomly found or unknown USB devices or cables and avoid public charging stations
14. Do not plug a USB drive or your phone into an untrusted computer

PASSWORD AND ACCCOUNT SECURITY

1. Do not memorize passwords! Store them!
2. **Use a different, unique automatically generated password for each login!**
3. Check if your passwords you use have been leaked, check at https://haveibeenpwned.com and https://haveibeenpwned.com/Passwords
    a. Use BitWardens feature for detecting reused or compromised passwords en masse.
4. Make sure they are ideally:
    a. Over 21 characters long
    b. Contain letters (upper case and lower case), numbers and symbols.
5. When you must remember a password, like for the master password in BitWarden.
    a. Come up with a full sentence you can remember (like a phrase)
    b. Randomly replace some letters with symbols, mixed upper case and lower case, and symbols
6. Use 2FA (two factor authentication)
    a. Most websites with logins allow 2FA, find this in the website's security settings
    b. Activate it and **save the backup code** in a secure place.
    c. Do not use SMS/text message authentication, this is insecure.
    d. Use Google Authenticaor app or Authy both are available on Android and iPhone
    e. Scan the QR code with the app.
    f. You will need to type in the numbers from the app every time you log in.

HOW TO TELL IF YOUR COMPUTER IS COMPROMISED

1. Unusual ads
2. Unusual slowdowns
3. Crypto locker messages, meaning.

    a. Files inaccessible
    b. Demand for a ransom to get your files back.

4. Any new software you do not remember installing.
5. New or unusual antivirus showing several viruses (fake antivirus are very common)
6. Emails or messages sent from your account that you did not send.
7. Any unexpected changes or anything "unusual" at all
8. Your web camera light is on when not being used, even after reboot.

IF YOU SUSPECT YOUR PHONE OR COMPUTER IS COMPROMISED

1. If any device is compromised, assume the device and all accounts ever used on it are also compromised.
2. Reset phone or computer (as listed above)
    a. This means REINSTALL THE OPERATING SYSTEM FROM SCRATCH
3. Change all passwords.
4. Reconfigure 2FA on all accounts.
5. Change master password on BitWarden.
6. There ARE NO SHORTCUTS
    a. It takes a while, but DO IT
    b. Do it RIGHT AWAY

MOBILE SECURITY

1. ONLY download and install apps from the legitimate app store.
    a. Ensure they are well rated and trusted apps from trusted vendors.
2. High ratings
3. High download counts
4. Verified apps are best.
5. Known vendors.
6. When in doubt, google the app and the vendor.
    a. Check app permissions! Do not install any apps that require unusual permissions or permissions you don’t think the app needs. Deny them!
    b. Make sure auto-update is on for all your apps and routinely check to make sure updates are installed.
    c. Beware security apps, antivirus apps, battery savers and memory savers. They do not do much at best and at worst are outright malicious.
    d. It is suggested you use the Firefox mobile browser instead of the default Chrome on Android, as it is a smaller target to be compromised.
7. Ensure your phone is encrypted! This is in settings.

    a. Ensure your phone is locked with a secure pattern or password! try not to use a PIN, these are often insecure.
    b. Face logins are very good on modern phones.
8. Always make sure you use a VPN on your phone, especially on public Wi-Fi
9. Do not turn on Bluetooth, location, Wi-Fi, or NFC unless you are using them.
10. Beware scam calls and texts! These are extremely common! Read about common scams and keep up to date with them!
11. Install the BitWarden password manager app, this will sync with the extension in your Brave browser to keep your passwords secure.
12. Change your voicemail PIN from the default.
13. Set up a support PIN with your cellphone provider, you will have to call them and verify your identity to do this. Some providers allow you to do this online in your account.
14. Always install updates for your phone operating system and apps when they're available.

Router / IOT Security

1. Find your router. it should be a box plugged into the wall that gives you internet.
2. Look on the bottom for a sticker describing the make and model of router.
3. Google for the manual
4. Follow instructions to log in and
    a. Change the default password.
    b. Ensure the Wi-Fi is using WPA2.
    c. Ensure port forwarding and NAT (Network Address Translation) is disabled
    d. Update the firmware.
    e. Ensure remote administration is disabled.
    f. Ensure NAT is disabled
    g. Enable the guest network for guests—do not give guests your real Wi-Fi password!
5. IoT (Internet of Things) devices can include.
    a. Amazon Echoes / voice assistants
    b. Smart lightbulbs
    c. Smart thermostats
    d. Smart plugs to turn on and off things.
    e. Printers / Scanners / Some fax machines
    f. Network Attached Storage (NAS)
    g. VOIP / IP Phones
    h. Any device connected to an app, computer, voice assistant or the internet.
    i. Any device with wireless connections
6. Go into the app for each device and update the firmware.

7. Use the router manual to isolate all IoT devices possible to their own subnet.
    a. Enable device/subnet isolation for any device possible.
    b. This will take some experimentation and "massaging" to get to work right without errors.
    c. Ideally, the IoT devices will be on their own wireless network, if supported by your router
8. Change any default passwords your devices may have.

Other Security Guidelines

1. US Military: https://public.cyber.mil/stigs/
2. US Government: https://csrc.nist.gov/Projects/United-States-Government-Configuration-Baseline
3. Payment Card Standards (PCI): https://www.pcisecuritystandards.org/security_standards/documents.php?association=PCI-DSS

Relevant Links

1. Current known vulnerabilities: https://nvd.nist.gov/ncp/repository
2. Check for leaked passwords: https://haveibeenpwned.com/
3. Scams and online security: https://www.consumer.ftc.gov/topics/online-security

Trusted VPN Providers

1. https://torguard.net
2. https://protonvpn.com (has a free package)
3. https://mullvad.net

Trusted Email Providers

1. https://tutanota.com/
2. https://protonmail.com/

Trusted Anti-Malware Programs

1. https://www.malwarebytes.com/ (paid)
2. https://www.bitdefender.com/solutions/free.html

To add to document

// non-face id login for win

// yubikey/master password on press/longpress/U2F/FIDO

// Glasswire/free alternative (?) https://safing.io/

// Threats

```
//			$5 wrench attack
//			Phishing
//			Malware/endpoint security
//			side-channel attacks
//		exchanges / “not your keys, not your crypto”
//			don’t store on exchange
//			exchange reputability
//		dapps
//			staking
//			investment
//			credit
//			leverage / margin / leverage coins
//			trust in dapp
// secure virtualized machines
// mywot.com
// tor browser
// GPG
//		masterkey generation
//			hardware wallet/U2F/yubikey
// VeraCrypt
// Box Cryptor
// Sky: Adnaseum, decetraleyes, sponsorblock, track me not
//		https://adnauseam.io/
//		https://decentraleyes.org/
//		http://trackmenot.io/faq.html
//		https://sponsor.ajay.app/ // debloat
//		https://christitus.com/debloat-windows-10-2020/
```

// https://www.oo-software.com/en/shutup10

// Step-by-step directions

// Screen shots

// Windows privacy/see sky