Kerno.biz LLC December 2016

How to Secure Your Privacy

Unfortunately, security breaches are commonplace these days and this can jeopardize our privacy. Hackers are gaining access to business computer systems everyday which puts our personal information in jeopardy. Every time we create a user name and password on a website or in an app we run the risk that the information stored behind that password will be stolen. So what are the steps we can take to help protect us?

Consumer Reports had an interesting article recently that lists a number of things we can do. Some of them were highly technical and only good for the do-it-yourself crowd, but here are a few highlights (plus I have added a few of my own):

- Don't use the same password on multiple accounts.
- Use difficult passwords with lots of letters upper and lower case, numbers and special characters.
- Use two factor authentication when available (when you enter a password a text message or email is sent with a code that you also have to enter).
- Don't use a simple PIN (1111 or 1234) on your phone or tablet. Don't use your birthday or last 4 of your Social Security number.
- Shred documents that contain your Social Security number, birth date, credit card number, financial account numbers, medical insurance numbers.
- Opt out of pre-screened credit card offers to reduce junk mail. Go to www.optoutprescreen.com or calling 888-567-8688.
- Reduce other junk mail at dmachoice.org.
- Reduce ads in your browser at www.aboutads.info/choices/.
- Stop ID theft after death. Send a copy of the death certificate to the IRS. Cancel driver's license, contact credit agencies, banks and

financial firms.

- If your mobile carrier offers PIN security, turn it on (place a PIN on your account that must be used to make any changes to your account).
- Watch your bills for unusual activity.
- Watch your kids credit reports. Kids are 51 times more likely to have their identity stolen.
- Every 4 months get a free annual credit report from one of the three main companies. That way you spread out over the year monitoring your credit report. Go to www.annualcreditreport.com or or by calling 1-877-322-8228.
- Consider placing a "Credit Freeze" on your account. Credit Monitoring vs. Security Freeze: A lot of people consider credit monitoring services that all these businesses are giving their customers to be too little too late. If you are not planning on opening any new accounts in the near future a much better strategy is to just freeze your credit file before something happens rather than simply being notified after something has happens. Transunion, Experian and Equifax are the three credit agencies.
- Change the default password for all your gadgets: routers, security cameras, baby monitors and anything else that is connected to your Internet.
- Use public WiFi as little as possible.
- When on public WiFi with a PC make sure you select "Public WiFi" if given the chance so your computer uses more security like turning off document sharing. On a Mac enter Stealth mode through System Preferences/Security & Privacy/Firewall/Firewall Options.
- Don't access financial accounts when on public WiFi.
- If you use public WiFi often, use a Virtual Private Network (VPN) to secure your connection to the Internet. Private Internet Access VPN is a good choice.
- Advanced: Turn on Encryption on your computer. Mac users: Go to System Preferences/Security & Privacy/FileVault. Windows Pro users: In Control Panel go to Bitlocker. Windows Home users: Download a free app such as GPG4win (aka Gnu Privacy Guard). Caution: if you turn on encryption do not lose your password or you will be out of luck. No one can recover an encryption password.
- Facebook Security:
    - Stop Facebook from tracking your cell phone. For an iPhone, you'll find the controls under Location Services. If you've got an Android device, look under Facebook Permissions in Applications Manager.
    - Turn on Login approvals (same as two factor authentication).
    - Hide your Facebook page under the "Who Can Look Me Up?" section.
    - Leave Groups by going to your Activity Log.
    - Reduce Ads in Ad Settings.
    - Hide your birthday, hometown, etc. in Privacy settings.
- Router Security:
    - Change the default password.

    - Change the default SSID (WiFi name) and don't use anything personal.
    - Use WPA2-AES encryption.
    - Update the router Firmware (routers have software too).

- If you are unsure if a website is safe or not you can check it's status at https://sitecheck.sucuri.net/. Right-click the link and select "Copy Link Address" then paste it in this website.
- Use browser extensions such as https://adblockplus.org/ (Ad Blocker) and https://www.eff.org/https-everywhere (uses https whenever possible).
- Beware of Phishing emails (email designed to trick you) that look like they might be legitimate emails. Any email asking you to take some action is a fake. If you have any question about any business you work with call the business directly using a phone number you already have. Don't click on links or call phone numbers in these fake emails.
- If anyone calls you on the phone claiming to be from a tech company, tell them to not call back and hangup on them. No legitimate tech company will ever call you.

I know a lot of these tips are highly technical so just do what you can. You can always ask for help and I would be happy to do some of this for you, understanding that a lot of this takes time. Stay safe!

More Information

66 Ways to Protect Your Privacy Right Now

A beginner's guide to BitLocker, Windows' built-in encryption tool

Newsletter Archives

Click here to read some of my past newsletters.

Some of my clients do not realize that my business has expanded to all mobile devices. In fact, any consumer electronic product that you can purchase I can help you with. So if you would like help setting up or syncing your new smartphone or tablet or connecting your new WiFi TV to the Internet, just let me know.

Claude Kerno
Computer & Consumer Electronics Consultant
719.650.9916
claude@kerno.biz - www.kerno.biz