United States Marshals Service

Eastern District of Virginia

Nick E. Proffitt
United States Marshal

Basic Cyber Security Recommendations for Executives

Judicial officers and other government and private sector VIPs should consider using some or all of these countermeasures in conjunction with a thorough physical home security survey conducted by a professional security team to increase their security away from the safety of their place of employment. These steps should be taken *proactively*, and not just in response to the receipt of a cyber intrusion, inappropriate communication or a threat to the protected person or their family.

- Use unlisted phone numbers and generic answering machine or voicemail greetings
- Receive "official" magazines/periodicals/papers/packages at work. Strongly consider a P.O. Box for your home mail if you are in a high-risk or VIP position. Mailings with your official title or position should not be delivered to home addresses.
- Depending on where you reside, you may not be able to simply use "name withheld" on land use records or deeds of trust. Some locations require a "Blind Title" to anonymize these records. Consider this when you buy or refinance your home.
- Request your local county/city Clerk of Court place an alert on your file to notify you or your security point of contact (Marshal) if someone attempts to place a lien on your real property.
- Be aware of MLS listings from the purchase of your current home- especially ones with "Virtual Tours" that were used when you purchased the home. Based on a cyber threat and a risk assessment conducted by our security team, the current availability of this information may justify a "blind title" be explored.

- Be aware of campaign donations and use of home address for these donations. These are readily available to data aggregation companies and associated software programs.
- Avoid social networking and blogging sites to the maximum extent possible -Do not post photos of you or your family anywhere on the web - **Advise family members of the security concerns about posting information and about you and your job.** Our security team can provide security briefings to family members if requested.
- Avoid "mixing" work e-mail with your personal e-mail - Never forward work e-mail to personal e-mail accounts or vice versa unless you use proper and approved encryption on both your work and personal e-mail accounts.
- Consider using secure and encrypted e-mail services like "Proton mail" or one of the many others for your personal email. These are oftentimes free (or donations accepted) and are very good. These services provide routine one-ended encryption and "end-to-end" dual key encryption with like company providers. Many also offer anonymized e-mail storage capability. They also offer secured VPN tunneled services for your personal home browsing for a very nominal fee. The e-mail platform on these secure e-mail services are very user friendly and resemble the "Outlook" e-mail software.
- Consider utilizing home based comprehensive cyber-security software packages with VPN capability as recommended by your security team or IT professional. (LifeLock, Norton Cyber, MacAfee Security are some of the many examples to choose from)
- Use strong and up to date anti-virus software on all devices. Clear cache files and cookies at least weekly and always use unique and complex passwords for personal accounts
- Strongly consider the risks when considering whether to "Opt-Out" of data mining sites like "Spokeo" and the many others. Oftentimes "opting out" of these data sites will actually increase your available personally identifiable information when the "opted out" company removes the information as requested, then sells your information to other sites that you have no control of. Bringing unwanted and sudden directed attention to yourself as a "VIP" or public official will also likely cause an increased chance of your information being listed on the "dark web" for sale or for more targeted negative action. Routine security monitoring and removal actions against dark sites utilizing "Tor browsers" and "onion routers" is very complex, costly, and such efforts have limited effectiveness for many VIPs in most cases.
- Avoid "storing" home addresses, phone numbers, or other personal, financial, or family information on web sites like Amazon, Ebay, Etsy, big box store sites etc.

- Don't use the "remember me" functions for usernames on financial and other important web sites you frequently visit if such sites contain your home address, phone number etc. Never use the "save password" feature on any web-based storefront.

- Beware of hazards associated with "Google-ing" your name from either your home or office computer-consider using the library or a hotel lobby for this, or better yet, allow your security team to do this for you when it is required. Use "Duck-Duck Go" for web searches or use a secure web browser as these tools do not store searched information or send information to third party advertisers. "Duck-Duck Go" allows an immediate wipe of searches when using their application on a mobile device.

- Prior to overseas travel, in addition to the normally provided travel security information, ensure that you receive a cyber specific briefing for the country you are visiting that addresses vulnerabilities and available countermeasures related to e-mail and web usage in the particular country you are visiting and those you will transit.

- Never use WiFi "Hotspots" (airport, hotel, restaurants) when conducting any web browsing that involves personal or secure data/passwords. Who owns the server that provides you the "free" access and where is their server located? Remember, nothing is really "free".

Once your information is out there, the chances of getting it back in any timely fashion is ***extremely slim*** due to caching of files and other storage methods which are almost immediate. In today's world, there is no such thing as "scrubbing" the internet for all your personal information and expeditiously removing that information. **Don't wait until a threat or IC is received to be concerned.**

I liken internet usage and cyber security to the old "*Whac-A-Mole*" carnival game...while all the moles must stick their head up at some time, the one mole that does so the longest usually gets "whacked".....***Don't be that mole.***