SOURCE

Prompts for Making Your Security Plan

Stephen Lovell, OpenNews Source (source.opennews.org)

- Working in news makes you a valuable target. Prepare accordingly.
- Be skeptical of security silver bullets and wary of black boxes.
- Consider paper or memory when you need extra security.
- Beware convenience and distrust default settings.

Common vulnerabilities and attack vectors to evaluate

- USB sticks. Always scan them, try to avoid them if possible, consider a burner machine just for opening them.
- Cables. Buy your own, don't borrow them.
- Password managers. They're convenient but provide a single point of failure.
- PDFs and .doc files. They're are often used to store malicious scripts. Be cautious with documents sent between devices.
- Flash and other browser plugins. Disable them or approach with extreme caution.
- Public WiFi. Very dangerous, get a portable VPN device or avoid altogether.
- Public charge ports. Avoid them.
- Any device you didn't personally buy, open, and set up. This is a classic black box scenario. In a work environment, this is hard to avoid, but be as careful as possible.
- Embedded URLs, particularly in email. Type them out or web search them instead of clicking.
- Embedded image display in emails. Turn it off by default.
- Auto-preview in email. Disable it. You don't want to auto-open something malicious because it is at the top of the list.
- Geotagging. Turn it off in all accounts and uploads, and consider stripping EXIF data from files for added security.
- Installation prompts, in browsers and elsewhere. Almost all are malicious, but they often look very real. Be suspicious of app updates—always read what they are doing and make sure the manufacturer has a matching update listed on their site.
- Ads. Yes, much of journalism relies on web ads, but ad networks are riddled with malicious ads that infect, redirect, and hijack devices and browsers. Consider blocking them or disabling both JavaScript and Flash.
- Printers. Never print confidential info on a public printer. Make sure your printer is secure and on a closed network or plugged directly into your machine. Printers can cache what you print for a long time, and are often wide open to attacks.
- Your resume. Many people keep these on personal sites as a PDF, and they often include addresses and phone numbers. Don't do this.

For more information, see "A Guide to Practical Paranoia," June 15, 2017

SOURCE

Representative ways to improve your security

- Scan ALL files using an up-to-date anti-virus app before opening them on your computer, always, no matter how tiresome or tedious.
- Buy your own networking hardware (router, and a separate modem) for your home. Don't rent from your provider, as theirs are often outdated.
- Consider not knowing your passwords. Try Off the Grid or write them down on paper in a secure location.
- Separate access email accounts from communication email accounts. Use one email account for account access and another for communication.
- Become familiar with privacy controls on all services you use routinely.
- Advise friends, family, colleagues, and acquaintances on your information-sharing preferences, and distribute private information to your contacts only with care.
- Don't save information in your browser. Never save passwords, credit cards, addresses, phone numbers, etc. in your browser. Type them each time. Never select "remember me" in login fields.
- Avoid using email clients outside of your browser, if possible. Email clients on your computer can be prone to being attacked more easily because they are outside the browser sandbox. (Mobile is a hard exception to not make here).
- Tape your computer camera and disable your device mic. Headphones in the jack sometimes accomplish this—you can test by looking at input levels.
- Turn your device's WiFi on and off manually. Letting it ping networks aimlessly can leak info about you, and in some tests can allow a device to be compromised.
- Keep Bluetooth turned off. Don't let it roam and leak data.
- Don't use Dropbox or other cloud drive services, especially as installed apps. If you need to use a cloud drive, consider the browser interface only. Since these apps sync files automatically, they could sync a malicious file in a shared folder from another person's machine.
- Get legal advice on Fifth Amendment protections and search and seizure laws as they relate to digital information and password protection. Save sensitive info in the way that is most protected by law.
- As an individual, consider whether you need a social media account. If so, strip it down to the bare minimum of data input, lock it down with privacy controls, and be aware of what is and is not visible.
- A personal website is a target. Hire a professional to help you secure your site or be very well informed.
- Manage your overall data presence. Remember that it's all one web, and thus all one data mine, whether or not you conceptually separate your personal and professional information.
- If you run a blog, consider switching to a non-archived newsletter for more personal information and writing. You'll never have complete control, but it's less indexable and accessible than a blog.
- Be careful about storing your digital signature on your computer in a document or as an image. Make sure it's secure.

For more information, see "A Guide to Practical Paranoia," June 15, 2017

Representative ways to improve your security, cont.

- Log out of everything when you're done, always. This reduces the possibility of your session being hijacked down the road.
- Use Two-Factor Authentication, but be aware that it isn't foolproof. Ideally, use a Ubikey for account authentication.
- Encode your answers for security questions instead of using literal answers. Many security questions are easy for a malicious actor to guess if you answer them correctly.
- Consider using the lynx text browser instead of a visual browser in high-security situations. It is not foolproof, but since it doesn't load plugins, JavaScript, or Flash, it can often be more secure.
- Consider using two different devices for work vs personal information, if you don't already. Consider using a dumbphone for secure situations. Never travel with a smartphone loaded with social media accounts.
- Treat every email as an investigation. If you get an email from someone with an attachment, or from someone you haven't heard from in a while, reach out via another means of communication to verify they sent it. Same goes for all other kinds of communication.
- Read the TOSes you agree to. This can be overwhelming and time consuming, but there are a few sections to look out for and be aware of. Mostly it's areas centered around data storage, retention, and sharing. Copy and paste the TOS into a text editor and search for key terms. The more information you pass to a site, the more important it is to do this.
- Make a disaster plan, and consider doing regular drills.
- Get familiar with the recovery process for all your accounts and services. Conduct regular backups and consider a safety deposit box for physical media.
- Educate yourself continuously. Sign up for some seclists and keep an eye on popular security and developer forums. They often provide a heads-up on vulnerabilities before they hit the mainstream news and the exploit goes extra wild.
- Look ahead. Organized crime data-mining and security-related AI prediction are happening and growing. Consider how your behavior may play into this, and plan ahead.