Security and Privacy Advice

Last edited: April 2nd, 2022

Desktop Hardware

On desktop, use a recent Windows Secured-Core PC, MacBook or Chromebook. These all have numerous security advantages, including proper verified boot, a strict IOMMU, etc.

Mobile phone hardware is covered in the mobile operating system section.

Operating System

Desktop

The desktop security model is very broken. It was not designed with security in mind — security was only a poorly implemented afterthought. However, there are some operating systems that are less bad in this regard. If you can, stay away from desktop and stick to mobile devices.

Use Windows 11 (preferably in S mode and on a Secured-Core PC), macOS, ChromeOS or QubesOS. Generally, these operating systems have made substantial progress on adopting modern exploit mitigations, verified boot, sandboxing, memory safe languages and so on.

There are advantages and disadvantages between these options, and it is not possible to give an accurate recommendation as to which of these will suit any particular person. One must develop their own threat model and choose the suitable operating system in accordance. For example, Windows 10 has great exploit mitigations, such as its coarse-grained, forward-edge CFI implementation, Control Flow Guard, whereas macOS has full verified boot to eliminate malware persistence.

Some of these operating systems do have some privacy invasive telemetry, but it can

usually be disabled in the settings and verified with a network analyser tool like Wireshark if you wish to be certain.

The security of QubesOS depends entirely on how you use it. The security within the virtual machines matter a lot — don't neglect it. Make sure that you use secure guest operating systems and split everything between as many virtual machines as possible. Virtualisation can be a very strong security boundary, but it is not magic. I'd recommend reading Brad Spengler's criticisms of QubesOS to understand some of its limitations.

Do not use Linux (QubesOS is not a Linux distribution).

Mobile

Mobile operating systems were designed with security as a foundational component. They were built with sandboxing, verified boot, modern exploit mitigations and more from the start. As such, they are far more locked down than other platforms and significantly more resistant to attacks.

Use either the stock operating system or preferably, GrapheneOS on a Pixel ≥4. Do not root your device, do not keep your bootloader unlocked and stay away from alternative operating systems like LineageOS, as they substantially worsen the security model. Read the Android article for more details.

Alternatively, use an up-to-date iPhone, which is comparable to GrapheneOS on a Pixel, and do not jailbreak your device.

Stay away from Linux phones.

Browser

For security, use Chromium. Avoid Firefox or browsers based on it, as they are currently very lacking in security. Microsoft Edge is a better choice for Windows users, as it can utilise Microsoft Defender Application Guard (MDAG) and has an enhanced security mode in which JIT is disabled and mitigations such as ACG, CIG, CFG and CET are all enabled in the renderer process.

For privacy, use the Tor Browser, and consider using the security slider. Do not assume that "hardening" Firefox or other browsers will make it private; it won't. Be aware that this has massively reduced security from other options, as mentioned above.

For a mixture of security and privacy, use Vanadium, Bromite or Brave, although none of these are as good as the Tor Browser when it comes to privacy.

Messenger

Use Signal, preferably with a burner or VoIP number.

Email

If you can, stay away from email, as it is a fundamentally insecure protocol, but if you must use it, use a reputable email provider with a strong focus on security, such as ProtonMail or Tutanota.

Consider staying away from web apps, as they can provide weaker security. When a user visits a website in a browser, that website can target that specific user with malicious JavaScript, whereas with a native app, the code is static. Additionally, apps can offer better protection against MITM attacks by pinning TLS certificates and removing the dependency on certificate authorities. This is commonly used in apps like ProtonMail, Signal and so on. However, websites in a browser are much less privileged, as they do not have direct access to system resources. Thus, using a web app could be more secure under certain threat models.

Passwords/2FA

Store passwords in a good password manager — KeePass or Bitwarden is recommended. Generate 20+ character passwords containing a completely random assortment of upper and lowercase letters, numbers and symbols. Use a different password on each website, and enable two-factor authentication (2FA) for every

website. Do not use SMS for 2FA, as it is vulnerable to simjacking and man-in-the-middle attacks. Use an authenticator app like Aegis.

Social Media

Don't.

General

- Do not put any sensitive information online if you can help it. If you must, use strong encryption.
- Always use full-disk encryption. Use Bitlocker on Windows, FileVault on macOS and dm-crypt on Linux.
- Do not plug your devices into unknown ports.
- Always update.
- Do not install a bunch of sketchy "security" software. Keep it minimal.
- Never leave your devices unattended.
- Always use HTTPS. Manually type in the `https://` part of the URL when visting a website to prevent sslstrip attacks. Make sure that the padlock icon is displayed in the address bar. Enable HTTPS-only mode in your browser.
- Install NoScript to block content such as JavaScript as much as you can. JavaScript inherently presents a massive attack surface, as it is arbitrary code executed directly from a website. NoScript also provides protection against attacks such as cross-site scripting, cross-site request forgery and more.
- Never visit unknown websites.
- Disable WiFi and Bluetooth when not in use.
- Use airplane mode and/or take out your SIM card as much as possible to prevent cell tower triangulation.

- Cover or remove any webcams or microphones.
- Do not give apps excessive permissions.

Go back