Privacy and Security Gifts

Rebecca Herold, Privacy & Security Brainiacs
2023 – 2024

1. **Comparatively low-cost USB data blockers**. Also commonly called juice jack blockers, to use yourself, and to provide to all your family, friends, and employees who work remotely. They are small and easy to carry in your pocket, phone case, etc. They look similar to this.
    They are also inexpensive. We've found them for as low as two for USD $7.89. They also typically cost less when buying them in bulk.
    NOTE: This is not an endorsement of this particular device over others. It is provided to show what one type of such device looks like.

2. **Personal portable charging devices**. Very useful for situations where a power source is needed, but there are none to be found, such as while hiking, or spending the day with a client in an environment with few-to-no usable electrical outlets. We carry two; one a flat credit-card size, and another the size of lipstick, that can each be put into different pockets, or storage belts. The charging devices vary greatly. A couple of types look similar to these.
    NOTE: This is not an endorsement of these particular devices over others. They are provided to show what two types of such devices look like.

3. **Charging-only cables**. Use these in public USB ports. This will prevent data from being transmitted through the USB connection similar to how juice-jack blockers work (but, yes, are larger and bulkier to carry). Cables that charge and provide data transfer have four wires within the cables. Charge only cables only have two wires within the cable, usually making them thinner.

4. **Electric outlet-to-USB adapters**. These are great for travelers. These are usually inexpensive (less than USD $10) and small. Most of these have two USB ports within them and look similar to this.
    NOTE: This is not an endorsement of this particular device over others. It is provided to show what one type of such device looks like.

5. **USB port blocker**. For example, here's a LINDY 40425 USB Type C Port Blocker Key. These devices physically prevent access to USB ports. A pack of 4 costs USD $35 - $40.
    NOTE: This is not an endorsement of this particular device over others. It is provided to show what one type of such device looks like.

6. **Fairly inexpensive cellphone temperature protection, padded, waterproof cases/covers**. Use these to protect your phone and devices from such temperature extremes and other environmental threats. While you're at it, get a case that also protects your phone from nearby wireless access via blue-tooth and RFID transmissions. These typically cost between USD $8.00 to $50.00
   NOTE: This is not an endorsement of this particular device over others. It is provided to show what one type of such device looks like.

7. **An RF-shielded travel belt, small storage bag, etc**. These are often called "Faraday bags." These can be used to store driver's licenses, passports, credit cards, and other RFID-embedded items. They prevent those nearby from accessing the data stored on the RFID chips; commonly called RFID skimming.

8. **Privacy screens/filters**: for smartphones, laptops, tablets, large monitors, etc. There are many different kinds and sizes. The cost varies based upon size. This one lists for USD $22.
   NOTE: This is not an endorsement of this particular device over others. It is provided to show what one type of such device looks like.
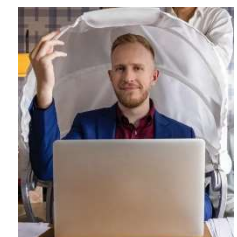
9. **Computer and work area privacy hoods/shades.** Extends beyond blocking the computer screen to blocking the view of a larger associated work area. The ones shown sell for around USD $35 – $100.
   NOTE: This is not an endorsement of these particular products over others. It is provided to show what a couple of such devices look like.

10. **UPS (uninterruptible power supply) devices** with surge protectors built in.

11. **Backup drives**. USB or hard drives that connect to your computer.

Privacy and Security Gifts

Rebecca Herold, Privacy & Security Brainiacs
2023 – 2024

12. **Cable locks**, to use while traveling, when working in a shared type of business space (e.g., rented work areas), when leaving the hotel room, in home offices where there are others in the house that do not live there, or when you don't want anyone to move your computing device. There are many different kinds. They run the gamut from USD $7 - $60. Here's one that is being sold for USD $20.
NOTE: This is not an endorsement of this particular device over others. It is provided to show what one type of such device looks like.

13. **Remote locator, data wipe and activity logging/recording tools**. The software package shown costs in the range of USD $20 - $30 per computer/device.
NOTE: This is not an endorsement of this particular software solution over others. It is provided to show what the screens of one type of such solution looks like.

14. **A physical alarm, or a software app alarm**, that will go off if someone takes the computing devices. There are many types, and they vary greatly in price. Here's a couple; one that sells for USD $11, and the other below it for USD $15.
NOTE: This is not an endorsement of these particular devices over others. They are provided to show what two types of such devices look like.

15. **Subscription to anti-malware** and other types of security and privacy software.

16. **Backup service subscription**. Make sure the service is one that has strong security and privacy practices. We also recommend using one that either has the option to store your data locally (where you are physically located, on a device you can disconnect from your network), or that they strongly encrypt all backups, and cannot decrypt the data (the subscriber controls the decryption keys).

17. **Encrypted USB drives**. To store copies of photos, videos, important financial papers and wills, etc.

18. **Covers for webcams**. These can be the items made specifically for this purpose, similar to the one shown. Or, working just as well, is a sheet from a sticky note cube/pad.

19. **Digital tracker detector** to check for digital trackers in your vicinity. For example, that may have been planted on your vehicle, in your bags, luggage, pockets, or other locations that you don't normally check that often. If you have a reason to believe you, or a friend or family member, is being tracked, invest in a digital tracker detector. There are many kinds. Ones similar to those shown below are typically available in the USD $40 - $50 range, and work well. Professional strength detector devices are available in the USD $150 - $250 range.

    NOTE: This is not an endorsement of these particular devices over others. It is provided to show what two types of such devices look like.

20. **Green screen with a background generator tool.** For use by those who do a lot of online meetings, schooling, etc. This will keep the work area environment where they are physically located (often in their homes) from being seen.

21. **Physical privacy screen.** We use these for our online meetings, courses, webinars, speeches, etc. They look exactly like the ones shown here. Of course, any type of physical, movable screen that is opaque will work. They vary greatly in price. We've found some as inexpensive as USD $15, and as expensive as USD $300. The ones we own cost USD $25 and USD $45.
    NOTE: This is not an endorsement of these particular products over others. It is provided to show what two types of such products look like.

22. **Portable VPNs** for work from home (WFH) folks, as well as travelers, students, and others who connect to the internet from remote locations.

23. **Privacy clothing**. A bit offbeat, but will definitely be used by some. Particularly travelers. For example, there are stores that make clothing that is "the first design collection that offers knitted garments that shield facial recognition," such as the item shown from Cap_able. *NOTE: This is not an endorsement of this particular store. It is provided as an example to show what one type of such clothing looks like.*

24. **Privacy glasses**. Used to fool facial recognition systems that use infrared and 3D infrared mapping/scanning. The type shown, Reflectacles, is in the range of USD $145 – $200. There have been several new types from other manufacturers emerging throughout the past couple of years. *NOTE: This is not an endorsement of this particular device over others. It is provided to show what one type of such device looks like.*

25. **Privacy scarves**. The examples shown from ISHU are being used by the rich and famous to protect their identities when they are in public being recorded by fans and paparazzi. Elements of the scarf are made of reflective materials that reportedly ruin photos and videos. These shown range from USD $365 – $456.

NOTE: This is not an endorsement of this particular product over others. It is provided to show what one type of such product looks like.

26. **Privacy make-up and hair**. Similar in concept to the privacy glasses. These use makeup and/or hairstyles to fool facial recognition systems. The ones shown are from CV Dazzle, and have been being created and evolving since at least as far back as 2010. *NOTE: This is not an endorsement of this particular product over others. It is provided to show examples of what these makeup and hair styles look like.*

27. **Privacy masks**. Face masks originally created and used in China to protect against smog are now starting to be seen throughout the world as privacy protections from surveillance cameras and facial recognition. Prices run the gamut from inexpensive to very expensive.
NOTE: This is not an endorsement of these particular products over others. It is provided to show examples of what these products look like.

28. **A one- or two-person privacy booth**. For home or at work. There are many options and manufacturers of these. They vary greatly. Here is one example of what is a stand-alone booth. We actually sent them a letter advising them that if they offered their privacy booths with embedded working blinds in/over the glass that would provide even more privacy.
NOTE: This is not an endorsement of this particular privacy booth over others. It is provided to show what one type of such device looks like.

29. **Two-factor authentication hardware**. There are several to choose from. A currently popular one is the Yubikey which looks like this.
NOTE: This is not an endorsement of this particular device over others. It is provided to show what one type of such device looks like.

30. **Offline (meaning your password can be stored locally) password manager**. We were asked to list some we like. None are perfect. However, three we like, for different purposes and in consideration of the ease of use and general understanding of technology by those using them include 1Password, Enpass, and Passwarden.
NOTE: This is not an endorsement of these over others. They are just some choices based on our work and what has worked well for our clients. Others may work better for your specific situation.

Rebecca Herold, Privacy & Security Brainiacs
2023 – 2024

31. **Microphone blocker**. This secures the computing device's microphone input. When plugged in, the microphone in the blocker will become the device's primary microphone and prevent others from listening in. Here is a popular one.
NOTE: This is not an endorsement of this particular device over others. It is provided to show what one type of such device looks like.

32. **For friends and family still using landlines, a call blocker**. Here's a popular one.
NOTE: This is not an endorsement of this particular device over others. It is provided to show what one type of such device looks like.

33. **Hard drive eraser**. Use these to irreversibly wipe out all data on a computing or storage device before you sell it, dispose of it, give it away, or repurpose it in any other way. Here's a popular one that sells for around USD $17.
NOTE: This is not an endorsement of this particular device over others. It is provided to show what one type of such device looks like.

34. **Shredding scissors**. For credit cards, paper, and other types of physical media that contains personal and other types of sensitive data. We recommend cutting twice, to cross-cut into tiny rectangles. These typically sell for USD $6 - $15.
NOTE: This is not an endorsement of this particular product over others. It is provided to show what one type of such product looks like.

35. **Shredding bin**. These are nice for at home, and for small businesses. This one finely cross-shreds 100 pages of paper at a time. These types vary in cost from the manufacturers. The type shown typically sells for USD $90 - $130.
NOTE: This is not an endorsement of this particular device over others. It is provided to show what one type of such device looks like.

36. **Voice changer physical tool**. Use to answer phone calls from unidentified numbers. Growing numbers of crooks are gathering voice recordings of targeted individuals to then use AI tools to call friends or members of the individual's family to impersonate the individual's voice and compel ransom or extortion payments from. There are many types of these voice changers. Some of the best ones are low-cost children's toys. But there are also high-end expensive tools available as well. A couple of the many possibilities are shown.
NOTE: This is not an endorsement of these particular devices over others. It is provided to show what two types of such devices look like.

37. **Voice changer software**. These are software that run on your phone and/or computer. Many of them are free, such as MyEdit, AudioDirector 365, AV Voice Changer, and Voicemod, just to name a few. They can be used during the same types of situations described previously. Sit with a friend, family member, or someone else to gift your time to implement voice changer software in their computers and phones.
NOTE: This is not an endorsement of these particular software over others. They are provided to start you on your software search.

38. **Artificial Intelligence (AI) detectors**. There are growing instances of AI using personal information of online posts and stolen information to train algorithms. There are also increasingly more instances of academic plagiarism and the use of stolen intellectual property (IP) for financial gain. To help identify such situations, there are increasingly more tools to help identify when AI created text, audio, video and images, many of which also indicate the original source. Brian Quinn and Erin Burns at Texas Tech University co-own, co-curate, and are maintaining a compiled list, "Generative AI Related Writing and Research Tools." This list would be useful for those who suspect their IP or personal information is being used by others. Sit with a friend, family member, or someone else to gift your time to implement AI detectors in their computers and phones. See it here:
https://guides.library.ttu.edu/artificialintelligencetools/detection#s-lg-box-31566533

NOTE: This is not an endorsement of this particular list and associated tools over others. It is provided as a possible starting point for those looking for such tools.

39. **Privacy protecting web browsers**. Tor, Onion, and many others (with associated wide variations of true privacy protecting features). These allow a wide range of anonymous online activities. Sit with a friend, family member, or someone else to gift your time to implement one of these privacy-protecting browsers.
NOTE: This is not an endorsement of these browsers over others. It is provided to show a couple of examples you can consider. Choose what best service your own personal context of use.

40.   **Universal Opt-Out Mechanisms (UOOMs).** In the US, in December, 2023, at least 7 states (California, Colorado, Connecticut, Delaware, Montana, Oregon, and Texas) have privacy laws requiring businesses to comply with opt-out preferences transmitted through UOOMs to allow individuals to opt out of targeted advertising and data sales. There may also be regulations outside of the US which also require such UOOMs. UOOMs include a wide range of computer and mobile phone tools engineered with the capabilities to automatically opt out of the sale or sharing of their personal information with third parties involved within the interactions. UOOMs transmit individuals' opt out preferences utilizing technical specifications, such as Global Privacy Control (GPC). Sit with a friend, family member, or someone else to gift your time to implement UOOMs in their computers and phones.

41.   *Security/surveillance cameras*. These can be privacy-invasive and/or privacy-protecting depending on the context of how they are used. To use them to protect your privacy, direct them within your personal/private space (home, vehicle, etc.). Set up alerts to send notifications when movements are perceived. There are literally thousands of these, from almost free to extremely expensive. Be sure to closely review the Terms of Use and the Privacy Notice. Many of these share the recordings made with third parties, such as cloud service providers, marketers, law enforcement, and government agencies. Before signing any agreements to use the cameras, make sure you've closely reviewed and understand what you are agreeing to.

42.   **Hotel/motel/rental room mobile privacy & safety door stopper/blocker**. Prevent being surprised by those entering your room without warning or knocking. And, to strengthen safety. Rebecca has traveled throughout the world. There have been some dicey situations early in her travels, and since then she always uses some type of door blocker. It is worth not only privacy and safety, but also peace of mind. There are many different types. Here are a couple of inexpensive types she uses, ranging in price from USD $4 - $12.
NOTE: This is not an endorsement of these particular devices over others. It is provided to show what two types of such devices look like.