APPENDIX D: Personal Privacy Practices

What does everyone need to know and how should they responsibly protect ourselves? Privacy policies should provide accessible procedures for users to limit or prevent information or image sharing and selling by the merchant, beyond pressing lawsuits. Start by examining how connected modern life is, with online exposure growing, from social media to the Internet of Things, with ubiquitous cameras.

[Have I Been Pwned] HIBP?

This is a commercial internet security website, known by the acronym, enabling consumers to check for data breaches on their personal information. It stands for "Have I been Pwned", colloquially pronounced have I been "poned", referring to password theft.

Social Media - R U There? (geolocation tracking)

Phone app location tracking can be altered in phone settings. Detailed advice is available, (Valentino-DeVries, Singer, Keller, & Krolik, 2018) .

Me/Not Me: Impersonations

Cell Phone: "sim-swapping" Scammers have been impersonating cell account holders and getting permission from service providers (sometimes acting as accomplices) to transfer phone service to another account. Text messages, emails, password confirmation codes, retail and financial account information all become accessible. Senator Ron Wyden, D-Oregon says "The industry is not exactly exerting itself, in order to better protect the consumer from these sim-swap scams." A wireless trade association, CTIA, formerly known as Cellular Telecommunications and Internet Association provides CTIAs Updated Messaging Guidelines and Best Practices, 2019).

Phone Calls: People are flooded by phone calls and automated robocalls, during election seasons and otherwise. Consider enrolling in the "National Do Not Call Registry." Callers may legally continue to call if you agree to accept calls. Don't reply "yes," even with an unrelated query, for example, "can you hear me?"

The Oregon Attorney General (AG) advises not answering calls you don't recognize and reporting suspicious calls, with details provided on the Consumer Protection, Fraud and Scams page. Callers can now spoof actual caller ID connections. A recent scam appeared to originate from actual County Sheriff's offices, listing the correct telephone numbers, but (criminally) demanding that funds be delivered and that callers "not hang up!." Details and email alert subscriptions are available from the Oregon AG Scam Alert Network for ongoing scams.

Phishing Emails: Our League state board and others report getting repeated emails and phone text messages asking, "are you busy- can you help?" These appear to be legitimate, registering with recognized names and contact photos but with other email addresses. A quick helpful reply will be answered with requests everyone has come to recognize, asking for money, gift cards, etc. A variant is asking "Grandma" for help, with the explanation, "I'd ask mom, but you know how busy she always is." If in doubt, check your contact files. You can block ersatz identity spoofing accounts, marking them as spam or reporting them as malicious, if need be.

Social Media "Me/Not me" Fake friend requests, if accepted, can hijack contact lists to spread maliciously and spread misinformation while masquerading with adopted identities. You may get suspicious requests, wondering-

weren't they already friends? Check for your actual friend in a fresh tab or window. Duplicate identities appear and spoofers may use actual photos copied from friends already in your lists. The spoof profiles are usually shallow, with only a few images, few if any friends, and a short account history with few posts. Privacy settings for legitimate accounts may look like this, too, so consider verifying in another way if you are curious. These can be sophisticated, targeted to appeal to interests reflected in posts. One conservative approach is to only "friend" those you know personally, or verifiable "friends of friends."

See further advice for all of these from Symantec.

What Does A Computer Problem Look Like?

Technology is evolving quickly and it may be hard to tell what is causing problems- outdated hardware or software, even user shortcomings. Getting advice intermittently is advisable. Here is some basic advice, starting with a summary from a computer manufacturer, Dell Customer Support (2019).

Install an antivirus program; keep it up-to-date and run scans regularly.

- Install an anti-malware program to block software from installing without the user's knowledge,
- Only download and install online software from trusted sources.
- Scan email attachments before opening the. Even images can carry a viruses.
- Don't trust cracked or hacked software. It often contains malware, Trojan horses.

Here are some symptoms to help diagnose malware:

- **Browser Redirects, Popups,** Homepage Changes: Browsers may suddenly redirect to unknown websites, or a previously set homepage may change without warning or input.
- **Slow Computer Response:** Computer may "freeze" or run slowly with regular use. Desktop operating system loading delays are common.
- Task Manager shows processes using 100%: Processor seems to work overtime and/or slowly. To check, press and hold down the CTRL + ALT + DEL keys at the same time. Then click the Performance tab. See process use in CPU Usage.
- Virtual Memory Low Message: This message will keep appearing no matter what changes are made to resolve the issue.

Note that this advice comes from Dell, a PC manufacturer. MacWorld cautions that Linux and MAC computers are also vulnerable and should be protected (Haslam (2019)).

Password Management

People manage many categories of services online, each with protected access. Consider the variety of accounts individuals sign into, easily running to hundreds of accounts per person. There are so many that managing password protection is highly advisable, with numerous programs available. It goes without saying that passwords should be varied, changed regularly, and never written in easily discoverable places.

- Personal records, for example work performance and pay, school, health care portals, professional society and civic memberships.
- Financial transactions, including banking, investing, bill-paying, purchasing
- Household apps: lighting levels, irrigation, dishwashers, security cameras, engaging and monitoring kitchen appliances
- Government services: libraries, the DMV, and others for licensing, social services, other agency information, like weather

- Personal communication networking between smart devices, linking laptop, phone, tablet, and watch, including phone calls and texts, emails networked social media and organization pages; blogs, membership/group pages
- Any websites that remember user preferences and history: media accounts, hobbies, file-sharing, travel and wifi access away from home
- Other online tools and resources: calendar and shopping list managers, some with enhanced performance for premium users with sign-in, managed accounts

Account passwords need to be difficult to guess, protected, for example with two-factor authentication, and changed regularly. Password management programs are available, to generate random, multi-character passwords, to protect, change, and retrieve them.

Use Diverse Passwords

A single computer can test 8.2 billion password combinations per second and "penetration testers" can use free software. System security officials assume that every website or service uses the very worst security practices imaginable. They assume that any password stored by someone else is effectively public. They advise never using the same password, or even remotely similar passwords, between any two services (Goodin, 2012).

Malware, Spyware, and Viruses, Oh My!

Applications and operating system updates are often patching security holes that would otherwise allow malware to infect computers. Monitor and install security updates.

Malware, or malicious software, can infect computers and spread over networks. Install protection programs and keep definitions current. Examples of malware include viruses, ransomware, spyware, Trojan horses, viruses, and worms, covered in the glossary. Adware is not considered malware unless it damages systems.

Google Download Option

Google offers a full user data download option. It could be a very large file, with everything already mentioned plus bookmarks, emails, contacts, photos taken with the phone, businesses you've bought from, calendar data, Google hangout sessions.

How to download your Google full info: https://takeout.google.com/?pli=1

Facebook Download Option

How to download your Facebook full info: https://www.facebook.com/help/212802592074644