BROWN

Stay Safe Online: A Five-Point Plan for Online Safety

patricia falcon - 2023-06-09 - Comments (0) - General Security

This article is packed with information on how to protect yourself when online. It covers five topics, each complementing the others and offering common sense practices you can easily adopt by using the associated tips and related resources. There is also a suggested LinkedIn Learning course at the end of this article for another way to learn to protect yourself.

1. Browsers & Search Engines: Adopt a “Safe and Secure” Mindset

Your browser and its search engines provide a hands-on connection to the Internet and all the services it offers. Your browser is also a primary target for cyber attackers who might, for example, be after the personal information you have unknowingly stored in it, or have hacked a site you believed was trustworthy. Your search engine may be telling more about you and your preferences than you’d like to share. Here are a few tips on how to protect yourself and privacy by adopting proactive safety behaviors and leveraging the security features of both.

Pro-Actions:

- **Keep your browser current by always using the latest version.**
  Make sure to enable automatic updating where this is an option. For others, simply restart your browser when you’re warned that a new update is available (don’t worry, all of your tabs and content will be there after the re-start).
- **Go stealth with InPrivate/Incognito browsing.**
  To protect your privacy, open an “incognito” or “private” window so you don’t leave a trail. Especially useful if you share your device with others, who won’t be able to see your activity. More details in **Configure Incognito Browsing**.
- **Use a private search engine.**

See **this related KB article** for more information.

- **Add an Ad Blocker.**
  Read **Browse More Safely with an Ad Blocker** to get started and for our suggestions.
- **Watch out for warnings.**
  If your browser warns you that the website you are about to visit is dangerous, close your browser tab and consult a different website for your content. You can also use **safebrowsing.google.com** with Chrome and other browsers to display a warning message before visiting a dangerous site or downloading a harmful app.
- **Take care with extensions/plug-ins.**
  While these can add functionality to your browser, they can also add vulnerabilities and need to be kept current as well. Add only what you need (especially for your Brown work) and remove them when no longer needed.
- **Curb your chat-time.**
  Only engage in online chats with known, trusted websites. Limit the information you share as you can't be sure who may be collecting it, what they are doing with it, and to whom they may be selling it or sharing it.
- **Close it out.**
  When you're finished with your session, close your browser.

Security Features:

- **Chrome:** **Manage Chrome safety and securely** (within Chrome, visit chrome://settings/privacy)
- **Edge:** **Privacy & Security** (within Edge, visit edge://settings/privacy)
- **Firefox:** **Browser Privacy and Security** (within Firefox, visit about:preferences#privacy)
- **Opera:** **Security and Privacy** (within Opera, visit opera://settings/privacy)
- **Safari:** **Safari Support**, **Change Security settings in Safari on Mac**

Related Resources:

- **Configure Incognito Browsing** (OIT KB article)
- **Use Private Search Engines** (OIT KB article)
- **Browse More Safely with an Ad Blocker** (OIT KB article)
- **OUCH! Newsletter "Browsers", Nov 2022** (SANS)

2. Smart Devices & Apps: Protect Your Devices and Data

Mobile devices have become a primary piece of technology for most of us, keeping us connected with each other and the world. It's not just the devices themselves, however, but the thousands of apps that make smart devices such a powerful and key part of our lives. For this reason, it is critical to pay special attention to your devices and their apps so that you get the most out of them as well as use them securely.

- **Secure your smartphone.**
  Here’s a checklist of recommended actions to take: Set up a screen lock; install a device locator and the ability to perform a remote wipe if it doesn’t come with these features; and use anti-malware software. See the Related Resources section below for a link to recommended malware removal and protection software.
- **Perform a privacy check-up on your smartphone to ensure apps aren’t collecting data they don’t need.**
  iPhone: Open Settings, then scroll down and tap the Privacy icon > Select a permission, like Calendar, Location Services, or Camera > Choose which apps should have access to that permission and remove the others.
  Android phone: Open Settings, then tap Apps & notifications, followed by Advanced App permissions > Select a permission and choose which apps should have access to that permission > Remove permissions for any apps you don’t want keeping tabs.
- **Use trusted apps.**
  It almost goes without saying, but don’t put anything on your phone if it doesn’t come from your app store (Apple or Google Play). Both perform a security check of all apps before they are made available. Android users need to be a little more careful when installing their apps, as they could enable certain options that allow you to download mobile apps from other sources.
- **Research an app before downloading it.**
  Has the mobile app been available long, or are you the guinea pig? How many people have used it, and what have they said about their experience? Who’s the vendor, and when did they last update it? The longer an app has been publicly available, received positive comments about it, and has a current update, the more likely it can be trusted.
- **Ask yourself if you need it.**
  Install only apps you need and use. Each app potentially brings new vulnerabilities as well as privacy issues (and takes up space). Also, if you stop using an app or no longer find it useful, remove it from your mobile device.
- **Configure the app's permissions.**
  Rarely do you get something for nothing. If an app is providing a great service and is also ad-free, what is the seller getting in return? Perhaps personal and geo-location details about you? When setting up an app, does it require access to your location, microphone, or contacts? If so, is it needed to perform the functions, and are you comfortable with this? When you set up permissions for the app, decide if you want to deny the permission request, grant permission only when it’s actively being used, or perhaps forgo it and look for a different app.
- **Protect your data by not sharing it in the first place.**
  Since most apps track at least a few things about you, the best way to keep your data private is to avoid sharing it. One way is to leave as many fields blank on your profiles as possible or even include fake information when not required and/or

relevant.

- **Don’t forget to update your apps**.
  Updates are released periodically to fix any detected weaknesses, so the more often you check for and install updates, the better. If your device allows you to configure your system to automatically update mobile apps, we recommend doing so.

Related Resources:

- **Secure Your Android** (OIT KB article)
- **Secure Your iPhone or iPad** (OIT KB article)
- **The Best Malware Removal and Protection Software for 2023** (PC Magazine)
- **Hackers, scammers and advertisers are after you – 5 smartphone security steps to take now** (Komando.com) (adapted for this section)
- **OUCH! Newsletter “Securely Using Mobile Apps”, Jun 2021** (SANS) (adapted for this section)

3. Transactions & Interactions: Safeguard Your Purchases

You can bank, make travel arrangements, order fast food, pay bills, window shop, and purchase just about anything, all online. No doubt that when you visit the mall, you leave unneeded credit cards at home, lock your car before entering the mall, and keep a close eye on your wallet or purse. Do you do the same with your online transactions? Here are some tips to protect yourself.

- **Use a computer/computer session dedicated to banking and other financial transactions.**
  If you don’t have a separate device to spare for this, you wouldn’t need to limit your available device solely to financial transactions. You could achieve this by rebooting the device before starting one of these sessions, then shutting it down again when finished. See “Go stealth with InPrivate/Incognito browsing” in the “Browser” section above for a related action you can take. Also, make sure the browser has been updated.
- **Watch out for fake online stores.**
  These can mimic the look of real sites or use the names of well-known stores or brands. It’s possible you may end up on one of these when you search for the best online deals. Warning signs are offers that seem too good to be true, or a “thin” website that doesn’t include details about the company or how to contact them. Play it safe by shopping from known and trusted stores.
- **Be wary of special offers from unknown sellers and read reviews of the sellers and their products before making a purchase.**
  Review the online store's policy on purchases from such third parties. When in doubt, purchase items sold directly by the online store, not by the third-party sellers that participate in its online marketplace. And note that, even with legitimate vendors, be

sure that you understand the seller's warranty and return policies before you make your purchase. Finally, if you're not sure about a company, even after visiting their website, search for the business name to see what others have said (look for terms like "fraud," "scam," "never again," and "fake") or see how they rate with the **Better Business Bureau**.

- **Keep an eye on your credit card statements.**
  This is a good practice wherever you shop. Review the statement for any suspicious charges, such as an unknown company or a very small amount. The latter could indicate someone has access to your credit card number and is testing access to your account by trying to charge an amount that might "slip under the radar" of the bank or yourself.
- **Enable the option to notify you by email, text, or app when a charge is made.**
  If you find any suspicious activity, report it to your credit card company immediately.
- **Use credit cards instead of debit cards for online payments.**
  Debit cards take money directly from your bank account; if fraud is committed, you'll have a much harder time getting your money back.
- **Electronic payment services or e-wallets such as PayPal are also a safer option** for online purchases, since they do not require you to disclose a credit card number to the vendor.
- **Avoid websites that only accept payment in cryptocurrency** or require obscure payment methods.
- **Use unique passwords for your different accounts.**
  Also, do not use your @brown.edu address as a contact or username for personal shopping.
- **Trust your Common Sense.**
  Stay alert, maintain a healthy suspicion, and take similar precautions online that you would when meeting strangers or shopping at the mall.
- **Make Wireless/Contactless payments even more secure.**
  See **section 5, Home Networks, Public Wireless, VPN & Bluetooth.**

Related Resources:

- **Federal Trade Commission Consumer Advice: Online Shopping** (FTC)
- **Avoiding and Reporting Scams** (FTC)
- **OUCH! Newsletter "Shopping Online Securely", Nov 2021** (SANS)

4. Social Media: Manage Your Online Presence

Communicating online can be deceptive. It's just you, a keyboard and monitor, so it can feel pretty private, even though that message could be broadcast to scores -- maybe hundreds or millions -- especially when using social media. Make sure to protect yourself and your

information with these recommendations.

- **Safeguard your accounts.**
  Lock them down with a strong passphrase and enable multi-factor authentication.
- **Review the privacy and security settings for any social media accounts you may use.**
  The more personal and private information that it might hold, the tighter you should make the controls. You should also periodically review these settings, as these may change over time.
- **Search yourself online.**
  Find out how much information and what types are already online. See the related resource for further suggestions.
- **Remember what (or who) the product is.**
  If a service is "free," then you are the product. Investigations have found that what you are doing online may be sold to others.
- **Careful with your use of location services.**
  Too much information about where you are could be used to harass or even stalk you.
- **Limit what you share.**
  Privacy settings alone might not be enough. Remember, the more you share -- and the more others share about you -- the more information that is collected and used by corporations, governments, and others. Plus, once it is “out there”, it’s like the proverbial toothpaste out of the tube. One of the best ways to protect yourself is to limit what you share and what others share about you, regardless of the privacy options you use.
- **Stay alert for potential scams.**
  As noted in the related article below, social media is an easy and low-cost method for cyber criminals to take advantage of millions of people. The three most common are: investment, romance, and online shopping (more on that later in this article).

Related Resources:

- **Use Facebook's Extra Security Features** (OIT KB article)
- **Protect Your Social Media Accounts** (OIT KB article)
- **OUCH! Newsletter “Top Three Social Media Scams”, Apr 2022** (SANS)
- **OUCH! Newsletter “Privacy - Protecting Your Digital Footprint”, Apr 2021** (SANS)
- **OUCH! Newsletter “Social Media Privacy”, Feb 2020** (SANS)
- **OUCH! Newsletter “Search Yourself Online”, Jan 2019** (SANS)

5. Home Networks, Public Wireless, VPN & Bluetooth: Secure your

connections

What does “online” mean to you? Is it what you see in a browser session? Is it a feeling you have when receiving a text from across the country? Is “online” a place, and if so, where? More importantly, how are you getting ”there”, and are you doing so securely? This section is about how you connect to “online”, which most of the time is through a wireless connection. Because you’re not fussing with cables, plugs and outlets, you might tend to forget about this less visible part of computing. The following tips will help to remind you and ensure that these connections are kept secure.

- **Secure your home WiFi.**
  Start by securing your WiFi access point (also called router) to limit who and what can connect to your home network. The five key steps you should take are:
  1. Change the admin password
  2. Create a network password
  3. Turn on automatic firmware updating
  4. Use a guest network (a virtual separate network that your WiFi access point can create), and
  5. Use secure DNS filtering. See the Related Resource “Securing Wi-Fi at Home” below for full details on each step.
- **Use public WiFi alternatives.**
  When away from home and you’re tempted to use an open WiFi hotspot, remember that you have no idea who configured the WiFi network, who is monitoring it or how, and who else is connected to it. One alternative is to use the personal hotspot feature of your smartphone for a trusted WiFi connection. If this isn’t possible, use VPN.
- **Install VPN on your devices.**
  Whether setting off across the globe, country, or town, make sure you’re installed VPN on your mobile device, because you never know when you may need a secure connection. If you are working on Brown business, use its VPN. Follow the instructions found in OIT’s **Virtual Private Network Knowledgebase folder** to download the appropriate installer for your device. See the Virtual Private Networks (VPNs) article in Related Resources for suggestions on how to select a personal VPN provider.
- **When not in use, turn off the juice.**
  This old adage can also be applied to those using Bluetooth or wireless on a device. If you’re not actively using the feature, switch it off. This leads into the next tip about protecting yourself against Bluetooth hacking.
- **Secure your Bluetooth devices.**
  There are a number of ways that Bluetooth can be hacked, bearing evocative names like “Bluejacking” (when hackers take over devices and send unsolicited messages to other Bluetooth devices), “Bluesnarfing” (gives hackers access to a Bluetooth device’s stored information), and “Bluebugging” (hackers gain control of a device’s

features, including making phone calls). The Bluetooth tips articles below include more details on the damage that can be done by a successful attack, as well as how to detect these (i.e., your device is less efficient, or you discover unexpectedly high data charges). It concludes with ten tips on how to protect your Bluetooth device, leading off with our already mentioned disabling it when not in use.

- **Make Wireless/Contactless payments even more secure.**
  While both Apple Pay and Google Pay tout the security features of their contactless payment options, they do suggest further actions you can take to protect dollars and personal data.
  Google Pay advises that you: always require your PIN, pattern, or password to unlock your device when it starts; only send money to people that you know; report unauthorized charges immediately; identify and report fraudulent Google Pay messages.
  From the article **Is Apple Pay Secure? The Platform Security and Privacy Overview**, the author has similar recommendations to Google's: do not share your passcode; do not allow others to add their biometrics onto your device; do not add cards on an unsecure Wi-Fi Network; act immediately if you have lost your device; keep your phone up to date; and enable two-factor authentication.

Related Resources:

- **Brown Wireless** (OIT KB articles)
- **Home Wireless** (OIT KB articles)
- **Virtual Private Network Guide** (collection of OIT KB articles)
- **Can Bluetooth Be Hacked? Bluetooth Security Tips for 2023** (Aura.com)
- **How Secure is Bluetooth? A Full Guide to Bluetooth Safety** (VPNOverview)
- **Wireless Connections and Bluetooth Security Tips** (FTC)
- **Bluetooth security risks to know (and how to avoid them)** (Norton)
- **Contactless Payment:**
  Apple Pay: Security and privacy overview | **Apple Pay security overview** | **Is Apple Pay Secure? The Platform Security and Privacy Overview** | **How Google Pay helps keep your data private** | **Manage your Google Pay settings** |
- **OUCH! Newsletter Top Cybersecurity Tips For Vacations", Dec 2021** (SANS)
- **OUCH! Newsletter "Securing Wi-Fi at Home", Jan 2021** (SANS)
- **OUCH! Newsletter "Virtual Private Networks (VPNs)", Jul 2019** (SANS)

Related LinkedIn Learning Courses (accessed through Workday)

- **Security Tips: Browsing the Web** (2021)
- **Securing Your Home Office** (2020)
- **Learning Computer Security and Internet Safety** (sections 3 & 4) (2022)

- **Working and Collaborating Online** (2020)