OWASP Consumer Top Ten Safe Web Habits

Safe practices for consumers on the web

How can you stay safe on the Internet? Surprisingly much the same you do in the real world. In this list, targeted for technical and less-technically minded users (Hi dad!), general habits are covered, as well as some specific steps you can take to increase your security and privacy and decrease your risk online.

Introduction

Today, more and more of our personal lives is spent connected to the Internet. We spend a significant amount of time checking email, looking at social media, logging into our financial accounts, shopping, and more. These activities expose our private lives to the internet where potential predators are stalking. Our personal computers are often connected to the internet 24/7 via high-speed data lines, wireless connections extend the boundaries of our houses, and now our home appliances are even exposed to the Internet through web interfaces.

We use these systems because it makes life easier. Where we once had to go to a bank to make financial transactions, they can all be done from the comfort of our home. We used to program our VCRs manually to record our favorite shows. Now we can simply open an application remotely and configure our TV or DVR to automatically record programs whenever we want. The internet has provided so many more conveniences to our lives but they don't come without risks.

These new technologies can also make life easier for the bad guys. Instead of breaking into your house, reading through your trash, or spying on you through an open window, tech savvy bad guys can effectively invade your privacy, steal from you, and generally make your life miserable from anywhere in the world. We often think that the danger is somehow different because it is computer based and not face-to-face; however, this is simply not true. How do we protect ourselves from tech savvy intruders? How do we protect our privacy and the privacy of our loved ones?

Guiding principles used to keep us safe in the physical world can also guide us in the computer world. We may not be aware of how computer attacks occur but we can look at "physical world" habits, which we apply without thinking because they're habits, and see how they apply to computers.

This document will cover ten habits we can use on our computers and provide recommendations to safeguard against common attacks. Each habit will provide a recommendation for all users and some recommendations for more experienced users. While the recommendations are specific ways the habits can be exercised, the habit themselves should remain valid, even when the computing landscape changes.

H1. Protect your secrets

Description: Passwords are a shared secret between a user and the system providing access and the most common way to authenticate to systems, applications, and services. Authentication is how a person or system proves their identity. Three methods of authentications are: provide something you know, something you have, or something you are. Passwords fulfill the first condition, something you know. People and systems authenticate by providing something only they know, therefore proving their identity. Weak password handling vulnerabilities are weaknesses in the handling, storage, and use of passwords. Many sites use security questions such as asking for your mother's maiden name when you want to reset a forgotten password. This practice has the problem that it often relies on easily guessable information and more importantly this cannot be changed if a data breach at a provider happens.

Threats: The exposure of passwords through mishandling or improper storage could allow discovery and use by attackers to access online services or data.

Impact: Weak password handling can result in the unauthorized access and compromise of data or systems.

Recommendations:

Consumers should focus on:

1. Use different passwords for each site
2. Use long passwords not based on a dictionary word
3. Don't share your password

Tech savvy users should also:

1. Use a password manager
2. Enable 2 factor authentication
3. Select fake and/or random answers for security questions

Example: Using an easily guessed password, such as 'Password' on your email account would allow an attacker to access your email. Even if it is not an account you actively used, it may be

used by accounts for password resets or as backup recovery emails. It could also be used to send email from an attacker under your name.

H2. Guard your privacy

Description: Everybody wants to ensure that personal and confidential information is only known to those that should know it and not strangers, the general public, or even attackers.

Threats: Information and data can be exposed not only through attacks but also through being careless or too open on social media or by unintentionally leaving information in documents such as EXIF data or geo locations in documents and pictures. You may accidentally reveal information you would rather wish kept private later.

Impact: Reputation loss, embarrassment, data breach, stolen credentials, and loss of domains or social media accounts

Recommendations:

Consumers should focus on:

1. Limit information shared on social media, including online “quizzes”, location, vacation plans, etc.
2. Use HTTPS; check your browser’s address bar for the secure icon
3. Check your privacy settings on all social media and mobile apps

Tech savvy users should also:

1. Delete/shred information which is no longer needed
2. Encrypt important information
3. Use Internet search engines which do not collect/retain search information for sensitive searches
4. Encrypt all your communications when browsing by using a VPN or browsers that have built-in proxy or VPN feature.

Example: Posting pictures or vacation plans openly on social media can inform bad guys where you are, if you may be alone, or if your residence is unoccupied.

H3. Use security software and services

Description: For added security protection, install and use security software. This of these services as security measures you would have around your house, such as a security screen door, smoke detectors, burglar alarms. Just as you would use products and services to add additional security to protect you in the real world, take steps to also protect your digital home.

Threats: The lack of basic security software and services could make it easier for hackers, malware, and viruses to attack your computer and gain access to sensitive information or destroy your systems.

Impact: Damage to your computer systems and devices. Unauthorized access to your data, accounts, and systems. Loss or altering of personal data.

Recommendations:

Consumers should focus on:

1. Enable the firewall on your personal computer and WiFi/Router
2. Install anti-virus software and IDS and regularly scan your computer
3.

Tech savvy users should also:

1. Use VPN
2. Use browser's plugins which enforce security
3. Use encrypted emails and messaging services

Example: Without virus protection, a file infected with a virus could execute on your computer, affecting your data or allowing the computer to be used in other attacks.

H4. Secure your environment

Description: Setting up your environment to enable security and maximize protections helps to defeat not only currently known attacks, but also help to thwart future, unknown attacks. Configure your systems and devices to enhance security features in the software or operating system.

Threats: Using unsafe configurations for devices and systems can make it easier for hackers to access or control your systems.

Impact: Compromise of your systems, allowing attackers access to your network, systems, and data. Revealing of personal and private data. Loss of access to systems and data. Altering of important or sensitive data.

Recommendations:

Consumers should focus on:

1. Change all default passwords
2. Disable guest accounts
3. Set your devices to ask before connecting to WiFi networks and remove networks no longer being used

Tech savvy users should also:

1. Configure your home devices (WiFi access points, Routers, TVs, etc.) to be secure (i.e., change default passwords, update firmware, rename routers and SSID's, turn off uPnP, etc.)
2. Configure your system to only use Whitelisted applications
3. Don't use administrator or system accounts for routine tasks/work

Example: Not changing the default username and password on a device, such as your home router or wifi access point, could allow an attacker to log into the system and the administrator and make any changes they want, including sniffing and logging your traffic, capturing passwords, or financial information.

H5. Perform routine maintenance

Description: Regular maintenance and upkeep is important for operating systems and software, just as it is for your car or house. In order to take advantage of patches to security vulnerabilities, more secure workflows, and general ease-of-use, update your systems on a regular basis. Or better yet, have updates automatically downloaded and installed everywhere possible.

As equally important as maintaining current software, uninstall software not used. It is not unusual for software to become vulnerable over time and neglected because it is no longer being used.

Threats: Out of date software can have security vulnerabilities publicly known for which there are easy and automated attacks. Software you don't use is more likely to suffer from neglect and become less secure over time. Additionally unused software needlessly provides more areas an attacker can attempt to exploit.

Impact: Systems, devices, and accounts which are unused or out-of-date can be exploited and lead to compromise of personal systems and accounts. This can lead to the disclosure of personal and private data, loss of access to systems, accounts, and data, and impersonation of your identity.

Recommendations:

Consumers should focus on:

1. Use current version of software and enable auto-updates where possible
2. Regularly patch your systems – Computers, phones, routers, WiFi, etc.
3. Use modern browsers

Tech savvy users should also:

1. Uninstall unsafe software, including Java, Shockwave, Flash
2. Uninstall software you don't use
3. Regularly run external port scans to check for unused services

Example: Unpatched systems are frequently targeted by hackers. A number of nasty, well publicized attacks could be prevented by keeping your system up to date.

H6. Think twice before trusting

Description: Many attacks such as phishing only work because user trust sources they should not, such a emails pretending to be from friends, online retailers, banks or others. Just as you wouldn't trust just anybody or anything in the real world, take the same care online.

Threats: Trusting untrusted sources can help attackers install malware on your devices or steal personal data.

Impact: Data loss, reputation loss, financial loss, data breach, credentials stolen, bank accounts lost, loss of domains or social media accounts, installation of unwanted software, malware, viruses, or other exploit kits and banning from the Internet if your IP becomes associated with illegal activities.

Recommendations:

Consumers should focus on:

1. Password protect your systems, devices, accounts, etc.
2. Question emails, even from friends and family and do not click on links from unknown users
3. If something doesn't seem right, ask the source directly or do some research (via Google or some other means) before taking any action

Tech savvy users should also:

1. Don't leave your systems unattended, use lockout screens
2. Use software from official web sites and app stores, do not give applications excessive permissions
3. Verify downloads against checksums

Example: We all get emails with links from people we know with broken english and a context that doesn't make sense. Or links to "Win a free iPad" or "Get your free $50 Amazon gift card." Don't click on them.

H7. Plan for the worst

Description: Disaster can always strike. The digital world is more, rather than less, likely to encounter a disaster. From hardware failure, to user mistakes (did I really just delete that???), to attacks by hackers, your data and systems will encounter a disaster, it's just a matter of time. Just as you would be sure to have a spare tire in your car, or candles in your house in case of a power outage, be sure to take proper step to be able to react in the case of a "digital disaster."

Threats: Disasters can be intentional, in the form or a hacker exploiting your data, accounts or systems, accidental, such as accidentally deleting valuable data, or acts of nature, such as flooding, fires, or lightning strikes (causing a surge in electricity which can destroy unprotected electronics).

Impact: Disaster can result in the loss and inavailability of important data, access to critical online accounts, and the inability to connect to the Internet.

Recommendations:

Consumers should focus on:

1. Backup important data, including passwords and encryption keys, and store in a safe place, offsite
2. Configure your devices to be secure, for example to use disk encryption, in the event they are stolen or lost
3. Use surge protectors

Tech savvy users should also:

1. Use online services and storage to backup data. Encrypt sensitive data
2. Print off account recovery sheets (i.e. Google 10 passwords) and store offsite at a friend's place or at the bank
3. Have backup Internet access

Example: Ransomware, which encrypts your hard drive and demands payment for the encryption key loses its power when you have a recent backup.

H8. Cleanup your devices and accounts

Description: Just as some people enjoy clutter-free, organized living spaces while some enjoy a more “livable” space, the same is true of your computers and accounts. You wouldn’t leave opened mail from your bank or stockbroker laying around the house for any visitor to look at. The computer is no different. Cleaning up after yourself reduces the places a nosey attacker can try to violate your privacy. There are many ways to clean up after yourself, but not all of them are obvious.

Threats: Leaving unused personal data, accounts, or systems accessible without protection can result in unauthorized use. Accounts left logged on after being used can lead to successful client-side attacks, such as CSRF, clickjacking, or XSS.

Impact: Data, systems, and accounts not properly secured when not in use can lead to the exposure of confidential data, unintended actions, destruction, or theft.

Recommendations:

Consumers should focus on:

1. Logout of accounts when you are done using them
2. Periodically review and delete online accounts no longer needed or used
3. Delete files no longer needed, including temporary files, text messages and chat logs, email (don’t forget sent mail), recycle bins, and old SSH keys

Tech savvy users should also:

1. Periodically review and delete system accounts no longer needed or used
2. Periodically clean your browser cache
3. Properly clean and sanitize computer equipment before discarding

Example: Logging into an online site on a friends computer, phone, or a public computer and not logging out allows others you may not intend to view your personal information and make changes to your account.

H9. Avoid unnecessary risks

Description: Avoiding dark alleys at night in the rough part of town when you're alone and have no business being there is generally a wise decision. Any possible reward isn't worth the risk. Just as there are safer places in your town or neighborhood, there are safer places to be on the Internet, and some less reputable places. Be aware of where those places might be and avoid them if necessary. If it isn't, take proper precautions to protect yourself.

Threats: Accessing unsafe or disreputable sites increase the possibility of attacks, being harassed, becoming a target of criminal or government interests, or the revelation of private information.

Impact: Damage to your reputation by being associated with certain sites, disclosure of visits in browsing history, or being targeted in ads on pages. Theft of personal and financial data.

Recommendations:

Consumers should focus on:

1. Avoid malicious/underground websites
2. Avoid creating accounts for "shady" and sites you do not use regularly
3. Do not do important tasks (pay bills, trade stocks, etc) on unprotected networks

Tech savvy users should also:

1. Use non-persistent virtual machines for riskier sites
2. When creating DNS domains, use a privacy service to hide your home address if you have an unlisted telephone number
3. Understand the risks of unsigned and side-loaded applications. Do not use them on your primary phone or system

Example: Having your email associated with an adult website and having the data breached. Having embarrassing bookmarks on your browser or in sites in your browser history when someone uses your computer.

H10. Be vigilant and on alert

Description: In the real world, being on alert is important. Hearing and investigating the strange noise your car is making now can save money in repairs later. Ignoring it could result in a car that is unsafe to drive. In the digital world, dismissing alerts and notification, casually responding to web page alerts, etc. can result in the compromise of your accounts, systems, and/or data. Learning what to be aware of and how to react (if at all) is important.

Threats: Missing early signs of possible security situations when they are preventable or limited in scope.

Impact: Increased damage, data exposure, or compromise.

Recommendations:

Consumers should focus on:

1. Think through online/digital activities and compare them to what you would do in the "real world"
2. Use account monitoring services
3. Review online account activity

Tech savvy users should also:

1. Beware of tech-support scammers
2. Be savvy on client-side and social engineering attacks
3. Use credit monitoring and freeze, and similar services to protect your credit

Example: Ignoring a web page that says you last logged in 2 hours ago from New York when you are in Seattle and haven't left the state in a year may be an indicator of breaches to come if you don't take corrective action.

Note:
I would like to suggest that OWASP illustrate this guide