

A person's hand is shown using a computer mouse on a desk. The background is a blurred office environment with other people working at computers. The text is overlaid on the image.

# OWASP CONSUMER TOP **TEN** SAFE WEB HABITS

SAFE PRACTICES FOR CONSUMERS ON THE WEB



# 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.

01



**PROTECT YOUR SECRETS**

# Recommendations:

## CONSUMERS SHOULD FOCUS ON:

- Use different passwords for each site
- Use long passwords not based on a dictionary word
- Don't share your password

## TECH SAVVY USERS SHOULD ALSO:

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

02



**GUARD YOUR PRIVACY**

# Recommendations:

## CONSUMERS SHOULD FOCUS ON:

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

## TECH SAVVY USERS SHOULD ALSO:

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

03



**USE SECURITY SOFTWARE  
AND SERVICES**

# Recommendations:

## CONSUMERS SHOULD FOCUS ON:

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

## TECH SAVVY USERS SHOULD ALSO:

- Use VPN
- Use browser's plugins which enforce security
- Use encrypted emails and messaging services



04



**SECURE YOUR ENVIRONMENT**

# Recommendations:

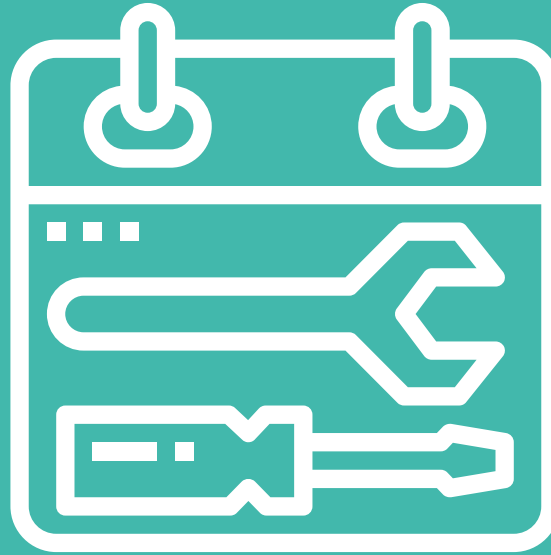
## CONSUMERS SHOULD FOCUS ON:

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

## TECH SAVVY USERS SHOULD ALSO:

- 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.)
- Configure your system to only use Whitelisted applications
- Don't use administrator or system accounts for routine tasks/work

05



**PERFORM ROUTINE  
MAINTENANCE**

# Recommendations:

## CONSUMERS SHOULD FOCUS ON:

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

## TECH SAVVY USERS SHOULD ALSO:

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

06



**THINK TWICE  
BEFORE TRUSTING**

# Recommendations:

## CONSUMERS SHOULD FOCUS ON:

- Password protect your systems, devices, accounts, etc.
- Question emails, even from friends and family and do not click on links from unknown users
- 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:

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

07



**PLAN FOR THE WORST**

# Recommendations:

## CONSUMERS SHOULD FOCUS ON:

---

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

## TECH SAVVY USERS SHOULD ALSO:

---

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



08



# **CLEANUP YOUR DEVICES AND ACCOUNTS**

# Recommendations:

## CONSUMERS SHOULD FOCUS ON:

- Logout of accounts when you are done using them
- Periodically review and delete online accounts no longer needed or used
- 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:

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

09



**AVOID UNNECESSARY RISKS**

# Recommendations:

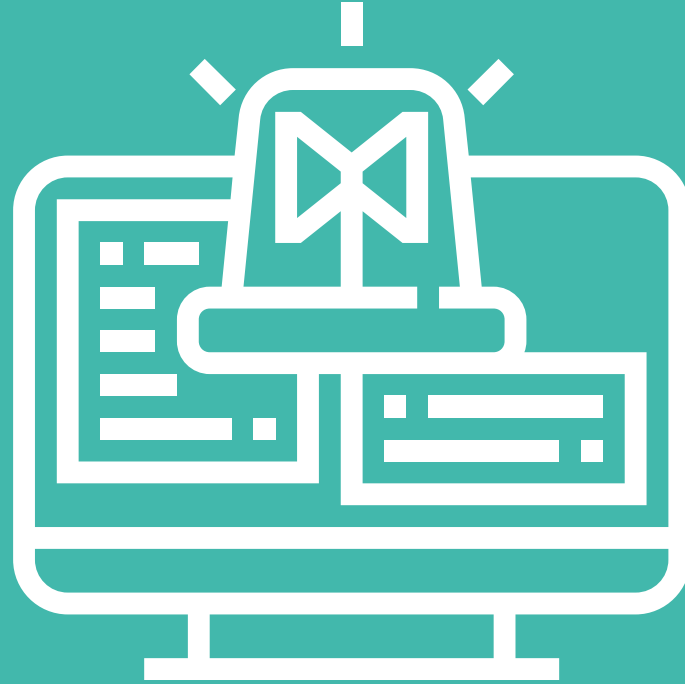
## CONSUMERS SHOULD FOCUS ON:

- Avoid malicious/underground websites
- Avoid creating accounts for “shady” and sites you do not use regularly
- Do not do important tasks (pay bills, trade stocks, etc) on unprotected networks

## TECH SAVVY USERS SHOULD ALSO:

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

10



**BE VIGILANT AND ON ALERT**

# Recommendations:

## CONSUMERS SHOULD FOCUS ON:

- Think through online/digital activities and compare them to what you would do in the “real world”
- Use account monitoring services
- Review online account activity

## TECH SAVVY USERS SHOULD ALSO:

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



# SUMMARY