CYBER OPSEC

Protecting Yourself Online

Think. Protect. OPSEC.

www.ioss.gov

INTERAGENCY OPSEC SUPPORT STAFF

INTERNET COMMUNICATION IN GENERAL

Our carelessness makes the job easy for the adversary.

The Internet was designed to withstand nuclear attack, not to be secure from its own users.

- Never assume security, assume it's unsecured.
- When security is needed, have trained IT security people in your organization seek and implement proper tools.

People can easily send fake e-mails that appear to be from people you know/trust.

- Always digitally sign messages.
- Encourage everyone else to sign their messages.
- In all cases (even with signed messages) personalize an e-mail enough so that it's obvious a real person sent it.
- Always verify suspicious messages before acting.

Even e-mails that are legit can be captured and read/modified in transit.

- Secure e-mails with digital encryption.
- Use file encryption or password protection if e-mail encryption isn't available.

Our carelessness makes the job easy for the adversary.

- If adequate protection is unavailable, don't send it over the Internet. Evaluate other options and work to get secure tools.
- If you have secure tools, actually use them. If you don't know how, find out. Laziness is the adversary's best friend.
- Don't let forwarded and repeatedly replied messages snowball. Eliminate the unnecessary data so a lucky adversary can't get the whole picture in one e-mail.
- Don't use CC to send e-mails to a list of people unless you specifically want everyone to see everyone else's e-mail address. In all other cases, send it to yourself (because everyone knows who you are already) and use BCC (blind carbon copy) instead.

BROWSING THE WEB

Clicking any link online tells the target Web site which site you just came from.

Cookies make shopping carts and online accounts work, but can be a risk in several ways.

- Delete cookies regularly or disable cookies through your browser. You can "whitelist" cookies from sites you need/trust while still blocking all others.
- Never use the "remember me" function on Web sites. This greatly increases your odds of having your account hijacked.

Companies want to know where you go online and use a function called "Web bugs" or "beacons" to do it. They look like ordinary images and are activated simply by viewing a Web page or e-mail.

- HTML bugs can only be blocked with special tools (hopefully being handled by your IT department).
- E-mail bugs can be completely blocked by selecting "text-only" in your e-mail settings or using an e-mail program that blocks images from untrusted senders.

Search engines track your search history and store it in databases; this can reveal a lot of information about you and your job in aggregate.

- Use generic information when possible (e.g., zip codes instead of addresses).
- Alternate search engines to improve your results and prevent a single engine from getting the whole picture.
- If you use related services, always log out before searching so they can't tie your results to your account (e.g., Log out of Yahoo! Mail before using Yahoo! Search).

Clicking any link online tells the target Web site which site you just came from. This can give away information you hadn't intended.

- When clicking links in search results, ask if any of the data (search terms) in your address bar give data away. If so, copy and paste a result's link to your address bar instead of clicking it.
- When posting links on a Web site you control, ask if you want to broadcast to the linked sites the fact that you linked to them. If not, print the links, but don't make them clickable so people have to cut and paste them instead.

BROWSING THE WEB

Installation warnings are the last chance you have to prevent bad code from getting into your computer.

Imposter sites will often mimic a legitimate site's URL through a common misspelling or by using another extension—like dot-com instead of dot-net. Get into the habit of typing Web site names into a search engine instead of the address bar.

- Many search engines pre-scan sites for malicious code and will warn you when you click them.
- Many anti-virus products have "site advisor" functions that provide visual warning icons for known bad sites.
- Search engines correct spelling, making it less likely you'll go to an unintended site.

Password security is key!

- Never use the same password from site to site. The owners of one site can easily try that name and password at other popular sites and see if it works.
- Never give any site any password for any reason. Most social networking sites ask for e-mail passwords while others ask for banking and credit card passwords. No matter how much they promise to protect and not misuse the information, history shows otherwise. The consequences of disregarding this rule can be severe.
- Look for the HTTPS in the address bar to verify that the transaction is secure—before entering your username, password, or any other important information. If it's not there, ask yourself if it's OK to broadcast openly and think twice before clicking the "submit" button.

Be cautious of fake alerts that look like legitimate warnings or system messages, but are not.

- Determine if the alert is real by closing all browser windows from the taskbar (don't click on or near the alert itself).
- If the alert remains, look to see if it mentions a Web site to visit or tool to download. If so, perform a Web search on the site or tool. If the results show that the site/tool is bogus, ignore the alert and ask your IT department to run virus and spyware scans on your machine.

Installation warnings are the last chance you have to prevent bad code from getting into your computer. They claim to be a "video player update" or "critical patch," but are often viruses.

- Say no to any "active-x" control or install warning unless you are sure of who created it, what it is, and what it will do once installed.

POSTING ONLINE

It is hard and often impossible to remove information from the Web…

Public visibility.

- Most things posted online are visible to everyone online (good and bad alike).
- Remember that even things posted "privately" often become public by accident or due to weak site security.
- Anything posted to your organization's Web site that's not protected by password or PKI authentication is publicly visible. Several other methods of protection are commonly attempted, but can be bypassed easily (domain restriction, robots.txt file, etc.).

Don't rely on third parties sites to keep information safe.

- Third party sites may have been initiated or infiltrated by adversaries putting your data at risk.
- Data centers used by these sites may be in other countries with weak data protection laws.
- Third parties are often hacked or sell user data outright.

Watch for metadata in files.

- Microsoft Office documents typically have a creator's name and organization in the file properties. This can be shut off in the options, but is usually on by default.
- Photos may also list names (if software was installed with the camera) and can also include GPS coordinates where the photo was taken. Photo editing software must be used to view and remove "EXIF metadata" in photos.

Photos often reveal too much.

- Buildings or natural features in the background can give away location.
- Reflective surfaces may show people, names, or other critical information.
- Photos of small animals or objects taken on a hand often provide palm and fingerprints to the adversary.

It is hard and often impossible to remove information from the Web after it has been posted, so be careful in the posting process before it's too late.

PRACTICE GOOD SYSTEM SAFETY

Remember that a password to a classified system must be handled as classified itself.

Keep your computer secure.

- Lock your computer when walking away.
- Don't use a government laptop on your personal Internet or at hotspots unless instructed by your security officer that you may do so.
- Don't leave laptops in hotels or cars unless it's unavoidable, but use a locking cable or hide them when you must.
- Make sure your laptop has full disk encryption installed before taking it out of secure spaces.
- Don't allow others to use your government computer without your direct oversight.

Be wary of devices.

- Don't connect any USB device, floppy disk, or CD to your computer unless it has been carefully scanned beforehand. Even store-bought products sometimes have viruses.
- Disable auto-run and auto-play functionality to help limit the damage a media virus can do.

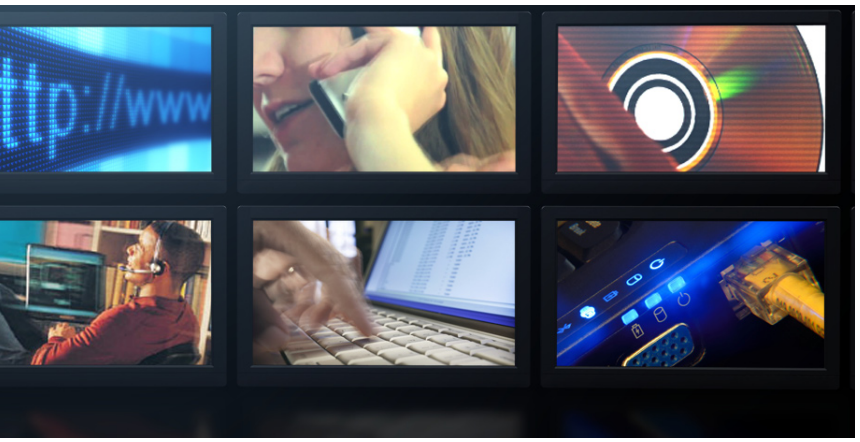
Dispose of media properly.

- Data recovery is very sophisticated. Learn and follow your organization's media destruction policy.
- Remember that nearly all devices have data storage. Treat any USB device (not just thumb-drives), floppies, CDs, phones, cameras, and hard drives as a disposal risk.

Practice good password safety.

- Don't e-mail or store any passwords unencrypted. Remember that a password to a classified system must be handled as classified itself.
- Don't put passwords on sticky notes or notepads unless you physically secure them.
- Learn how to create hard to guess, but easy to remember passwords and change them often.

PROTECT YOUR PORTABLE DEVICES



Many portable devices (phones, laptops, earpieces) include wireless capability, but not security.

Wireless allows adversaries to connect at distances of up to a mile or more.

- Your movements can be tracked.
- Stored or transmitted data can be stolen.
- Stored or transmitted data can be modified.

Many portable devices (phones, laptops, earpieces) include wireless capability, but not security.

- Turn off wireless if it's not necessary.
- If security is present, learn and activate all security features appropriately.
- Remember commercial security is weak and shouldn't be relied on in most cases.
- When in doubt, pull the battery (where able) and put the device in an RF shielded container.
- Always first ask if portable devices are necessary for your mission. They're no risk if they're not used.

Portable wireless (particularly RFID in badges) can be used for individual identification. These devices must include strong authentication and encryption to deter these risks.

- Copying at a distance thus invalidating their use for keyless entry systems and personal identification (such as with US passcards).
- Tracking your movements.
- Triggering cameras or even roadside bombs targeted for individuals.

Portable devices are easily lost or stolen.

- Always encrypt important data.
- Put strong lock-codes and passwords on your devices to prevent tampering.
- Keep them secure and out of adversary hands.

“It is vital that we all understand that even information that is UNCLASSIFIED is still important and in need of proper protection.... The information we put out there is immediate and forever and it is incumbent upon all of us to strongly consider that before putting anything out in the public domain.”

—LTG Keith B . Alexander, USA
Director, National Security Agency
Executive Agent for Operations Security

Think. Protect. OPSEC.
www.ioss.gov

INTERAGENCY OPSEC SUPPORT STAFF