Surfing The Web

The WWW (*Wonderful Wide World)* of Information

Tour of your browser:

Menu Bar

File

New Tab, New Window, Print Preview, Send

Edit

Find on this page

Favourites

???? Moving titles for priority

Tools

Delete Browsing History, Pop-up blocker, **Internet Options**

Surfing the Web General:

Risk	DOs	DON'Ts
Virus Worms Trojan Spyware Malware	Validate the website you are accessing Install personal Firewall Be cautious if you are asked for personal information Use encryption to protect sensitive data transmitted over public networks and the Internet Install anti-virus, perform scheduled virus scanning and keep virus signature up-to-date Apply security patching timely Backup your system and data, and store it securely	Don't download data from doubtful sources Don't visit untrustworthy sites out of curiosity, or access the URLs provided in those websites Don't use illegal software and programs Don't download programs without permission of the copyright owner or licensee (e.g.

Do's & Don'ts Of using social Networks:

Be selective when adding friends

Don't publish information that identifies you.

Chose sensible, strong, hard to guess passwords

Never use inappropriate language

Stop & think before you click

Don't make your online presence all about you.

Use a fully protected computer

Don't upload inappropriate pictures

Know the privacy settings

When downloading apps don't give them permission before verifying

---

DO

- Use a **strong password**.
- Use **privacy settings**. Insist your friends use theirs too.
  - NEVER leave anything but the bare minimum as publically available. Make sure only your accepted friends or followers can see what you put up.
  - Even then **leaks, hacks, and privacy policy revisions are not unheard of**. Don't assume what you do post IS secure, despite the settings.
- Use **HTTPS** to connect to your social networking sites whenever possible, especially when connecting from a public hotspot. Be wary if your social networking service only uses HTTP for login credentials only.
- Whenever possible, **organize contacts into "categories"**.
  - Most of us do this between friends and family anyway, but from a security standpoint it might also make sense to separate "best friends" from "person I met yesterday afternoon"
- **Verify** friend/follower requests.
  - Don't accept just anyone. Most scams start by someone bluffing their way onto your friends list. KNOW who you're sharing your information with.
- **Verify links, attachments, downloads, emails, anything sent to you**.
  - Even your trusted friends could've had their accounts hacked. Don't wire that "emergency money" until you can voice-verify.
- Investigate exactly **what information any third-party add-ons, games, extensions, etc. will be privy to**.
  - Does that poker game REALLY need access to your contacts list?
- Read up on the security tips and instructions provided by the Social Network itself, as well as what trusted security professionals and sources have to say.

DON'T

- Give away your password or use the same password for any other services.
    - If a leak at Facebook causes your password to become public, you don't want a hacker being able to use that same password to log into your Gmail or Courseworks.
- Put in any more information than you absolutely have to.
    - You should never put in more information about yourself than absolutely necessary. Hackers, scammers, stalkers all use that information to do anything from guess answers to your security-questions, to impersonating you when trying to scam another user.
    - On that same note, be careful how much live information you're putting out there. Don't advertise when you're going on vacation, when your possessions might be left unattended, that super expensive thing you just left the store with, etc.
    - Also be aware of auto-geotagging. Some services will automatically tag your status updates with GPS information. If you don't want everyone to know where you are, make sure your social networking service doesn't turn on this "feature" for your "convenience" automatically.
- Upload anything you wouldn't want **everyone** to see.
    - Assume that anything you put up will be revealed to the internet at large at some point, whether through hack, leak, or privacy policy change.
    - Nothing is ever really gone from the internet. Even if you delete a picture from your account, it's still sitting on Facebook's server somewhere.
    - In a professional setting, be mindful of inadvertently letting slip sensitive information that could harm your company or get you fired (new security software, procedures, etc).

Do’s & Dont’s When Travelling

1. **Don’t connect to the wrong network (it could be a trap)**

   When you’re staying at a hotel, take a second to ensure you’re actually connecting to the hotel’s true Wifi network and not one with a similar name that’s designed to trick you (i.e., “Hotel Guest Wifi”). Hackers routinely set up these decoy networks, waiting for someone to take the bait and connect. Once you do, they have the ability to see everything you’re doing online (and depending on your firewall protection, access your computer’s entire hard drive). Always consult the front desk and have them provide the network name and password.

2. **Don't assume Wifi is "protected" because you typed in a password.**

   This one is the most shocking to frequent travelers. Most people have enough basic cyber common sense when surfing on public Wifi hotspots (like a hotel lobby or rooftop), but what they don't know is that just because a hotel requires you to type in a password to access the Internet, it doesn't necessarily mean the network is any more secure. Typing in a password is merely an authentication process—guests could still be signing onto an open network. (To check if the Wifi network is secure, look to see if there is a "lock" symbol next to the network name, which provides more safety than if not).

   Even on a secure network, with the way most hotel networks are configured, anyone that is signed into that same Wifi network with a password is on the same network and thus, could potentially hack into your computer, gaining access to passwords, credit card numbers and personal information.

   The only way for a hotel to truly protect their Wifi users is to segment their network traffic (like we do), but at this time, many do not utilize that technology. So then, how to protect yourself if you find yourself on a questionable hotel Wifi network…?

3. **Do take simple precautions like Firewall Protection.**

   Hacking doesn't just mean someone can grab your online information. If you don't have Firewall Protection, a hacker can access your *entire* computer hard drive (including cached credit cards and passwords). Luckily, enabling firewall protection is simple (just a click of a button) and doing so essentially eliminates the hard drive threat.

   (To enable firewall protection, go to Control Panel on Windows or System Preferences on Mac. As an extra precaution, make sure your firewall protection software is up to date before traveling.)

4. **Do Disable File Sharing.**

   Sharing files or any activities where two computers talk to one another (like music sharing between you and your spouse's computers in a hotel room) is one of the riskiest things you can do over hotel Wi-Fi (or any public network for that matter). By default, most laptops have file sharing turned on, so take the extra step to specifically turn it off in your "Control Panel" settings on Windows or in "System Preferences" on a Mac.

5. **Don’t perform any money transactions on hotel Wifi. Period.**

   Avoid logging into your online banking account or doing any type of online shopping, money transfers or transactions…you’re making it way too easy for a hacker to get your passwords or credit card info.

6. **Don’t assume “https://” means your transaction is secure.**

   This one is another shock for the savvy cyber travelers out there. “Https://” indicates that the data transfer between your laptop and that particular website is secure *on their end of the site.* But it doesn’t mean someone can’t hack in on *your* end. In other words, if you’re at home on your own personal, secure Wifi network, then a “https” is a great sign — it means you’re doing business with a verified, secure site, but if you’re on a compromised network (like a hotel with open Wifi), you’re still vulnerable.

7. **Do feel free to use Wifi for “safe” activities.**

   Relax in your hotel room and use your Wifi for benign activities like reading blog posts or news from websites you’ve visited before and know are legitimate. Streaming is also fine, as long as you’re using services and websites that you’ve used before and trust (like YouTube). But beware, every time you manually type in a password, someone could potentially be tracking it. And if you see a pop-up for a new version of Adobe, don’t take the bait. Wait to do any software updates until you are in the privacy of your own home (and Wifi network).

8. **Do sign off from the Internet when not in use (or turn your computer off).**

   Staying signed into the Wifi indefinitely (which most hotel guests do, leaving it on for the duration of their stay) means you’re giving hackers a lot more time to access your computer (they can only access it when you’re online). Turning it off or putting your computer in “hibernate” mode will eliminate their ability to do so.

9. Do ask questions before you book a hotel.
For those guests looking to be the most proactive about their cyber-safety, consider taking into account the type of Wifi network a hotel has before you book. “At hotels that we provide Internet for, we segment and encrypt the traffic so that other users on the network can’t access it,” Salas explains. “Those are the key words you’re looking for when you call and ask a hotel about their network.”

Maintenance & Security

Tools > General> highlights