

## Questions from Prof. David Read

Friday, October 16, 2020 7:00pm EDT

---

### **If I clear my cookies after I finish my session, am I safe or are the cookies still out there?**

*Submitted: Catherine S. P'21*

#### **ANSWER**

Clearing your cookies helps prevent sites from identifying and tracking your activities as you access different sites. It is not the only way your activity may be tracked but is a step in the right direction. Note that clearing a cookie does not remove information from a web site's database. If you visit the site again, and it is one that requires you to provide a user name (and usually a password), the site will typically recreate the cookie.

### **What internet browser do you prefer?**

*Submitted: Russell P. P'23*

#### **ANSWER**

I use both FireFox and Chrome. They each have added security features, such as blocking tracking cookies, and each releases new versions to address security concerns fairly frequently. My main reason for using these two is because I go between different computers and operating systems so the ability to synchronize tabs between different computers is helpful.

### **How do individuals encrypt their data?**

*Submitted: Regina C. A'74*

#### **ANSWER**

You can encrypt the hard drive on your computer fairly easily with Windows, Mac iOS, or Linux. If you use Windows Professional Edition the tool is called BitLocker. If you use Windows Home Edition the feature is called device encryption. On Mac iOS the feature is called FileVault. On Linux the typical way to encrypt is to use Linux Unified Key Setup (LUKS), though there are a variety of tools available for Linux disk encryption.

One important caveat: if you encrypt your hard disk you **MUST** backup your disk to another disk (external drive is the typical approach). This drive should also be encrypted with a different passphrase. The reason for having backups is to address the fact that it is impossible to recover information from an encrypted disk if you forget your passphrase or if the disk suffers a failure.

### **Is it insecure to save your password on the computer or use "keep me signed in"**

*Submitted: Scottie Hall P '24*

#### **ANSWER**

Short answer for both is yes, for different reasons. Saving your password (unencrypted) on the computer leaves you open to someone stealing the computer, or installing malware that steals files, and obtaining your password. The "keep me signed in" option means that if someone gains access to your computer, or installs malware that steals files (in this case stealing the cookie with the remembered information), they can use that stored login to access the site as you.

One option for password simplification is to use a password manager. This is a program that stores your login and password information for each site. It can also generate strong passwords for you. This makes it easier to maintain separate passwords for each site, which is important. The password manager uses a master password (passphrase) that you supply. It then encrypts all your other passwords. The master password is the one password you have to remember. You want it to be a really strong password since it is protecting all your other passwords.

### **How does a casual user encrypt data at rest for home uses?**

*Submitted: Russell P. P'23*

#### **ANSWER**

You can encrypt the hard drive on your computer fairly easily with Windows, Mac iOS, or Linux. If you use Windows Professional Edition the tool is called BitLocker. If you use Windows Home Edition the feature is called device encryption. On Mac iOS the feature is called FileVault. On Linux the typical way to encrypt is to use Linux Unified Key Setup (LUKS), though there are a variety of tools available for Linux disk encryption.

One important caveat: if you encrypt your hard disk you **MUST** backup your disk to another disk (external drive is the typical approach). This drive should also be encrypted with a different passphrase. The reason for having backups is to address the fact that it is impossible to recover information from an encrypted disk if you forget your passphrase or if the disk suffers a failure.

### **Is it too late or impractical to reinvent the World Wide Web platform to one that has security designed in to the foundational structure that will eliminate the basic vulnerabilities you've outlined?**

*Submitted: Roy F. P'23*

#### **ANSWER**

Sir Tim Berners-Lee, who is credited for inventing the WWW, has been frustrated by the ways the platform is used for ill intent. He has started an effort to address some of the shortcomings but it is not easy, The underlying protocols cannot be changed without breaking current web sites and browsers. Here is his call to action: <https://webfoundation.org/2019/12/i-invented-the-world-wide-web-heres-how-we-can-fix-it/>

### **What will the impact of quantum computing be on cyber security measures?**

*Submitted: Greg F. P'22*

#### **ANSWER**

If a reliable quantum computing environment is created our current encryption approaches will become ineffective. We've seen this on a smaller scale as computers have become faster over the decades. Encryption that worked well in the 1970s is easily broken in seconds using a modern laptop computer. However, new algorithms (ciphers) and longer key lengths have been used to maintain a reasonable level of data protection. The arrival of quantum computing will require further work to create ciphers that protect data under these new conditions. Work of this nature is ongoing and is a fascinating area of research.

### **What if we don't accept a cookie when asked on a site, especially if we can still access the site?**

*Submitted: Regina C. A'74*

## ANSWER

Generally the site will not work correctly unless you accept its cookies. There are third party cookies, used to track your access across multiple sites, that can often be rejected without a problem. Newer browsers have a “do not track” feature that will look for these “beacons” and reject them automatically.

Opening an incognito browser each time you go to a site is one way to reduce the amount of tracking a site can do without losing all the functionality. However, some sites, such as news sites that offer a few free articles, will refuse to allow access from an incognito browser, since they would not be able to limit your article access in that case.

**As cloud grows in popularity, should we expect cloud providers to play an active role in helping with vulnerabilities? They seem to own at least load balancing, and many other critical infrastructure. Are we heading to a slightly safer Internet, or does cloud just means a centralized place that could be taken down and the whole Internet service will shut off for a region?**

*Submitted: Vu N. A'17*

## ANSWER

Cloud, at least at this point, adds more risk in several ways. The co-location of different organizations' applications and data make it a more attractive target to an attacker. If the attacker finds a weakness in one company's cloud configuration they may be able to leverage various attacks against the hosting company's software (the hypervisor) to access other organization's cloud-based systems. Also, attacks targeting computer hardware (the processor for example), could allow the attacker to access data from all the companies sharing that cloud server.

Another shortcoming I've seen with cloud security is that people setting up applications on the cloud aren't always trained in infrastructure management and data security. They don't have the background to understand implications of certain server configuration options. The cloud vendors may have different tiers of service, with security-based services being quite expensive. This leads to organizations choosing cheaper service tiers believing they can manage the configuration themselves.