THE UNIVERSITY OF CHICAGO | Biological Sciences Information Security Office

**December 2022**

# Cyber Security Awareness Newsletter

**Protecting yourself and information from cyber security threats**

The December holidays is when a lot of folks create "New Year Resolutions." In this December newsletter I want to give you some ideas on Cyber Security New Year Resolutions that can help keep you safe. Before we jump into that, I want to make everyone aware that the last week of January is data privacy week, and we are currently polling interest in a BSD departmental and individual hard drive destruction "Shred-it" event. If you are interested, please let us know how many hard drives you would be bringing. E-mail us at security@bsd.uchicago.edu

**Resolution #1 Password Overview – A Password Manager**

Sometimes it is worth reviewing our password use and creation strategies so that we can make a few changes to help make our passwords harder to crack and put us less at risk.

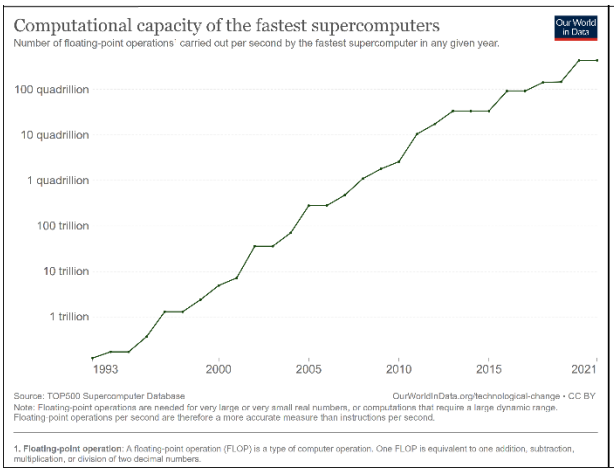
- Are you using the same password for your bank account, PayPal, Venmo, Google Pay, Square, Apple Pay, Amazon Pay, your personal e-mail account, as well as your work account, personal computer account, etc. ?
- Do the passwords you use contain elements of personal details such as birthdays, your hair color, favorite food, etc.?

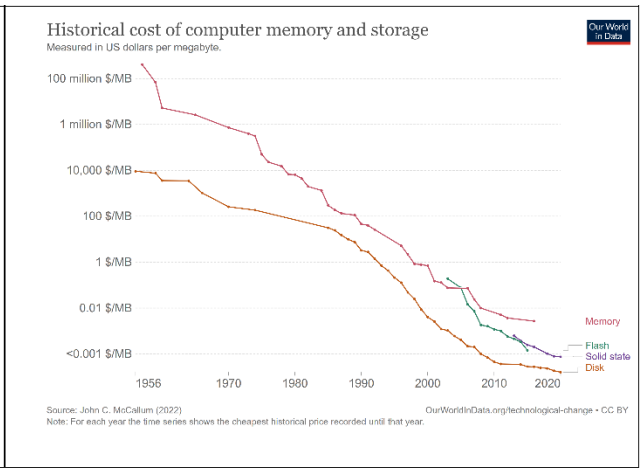
Using the same password on multiple accounts or using passwords with personal detailed information can put you at risk. This gives malicious users easier access to your whole digital life and make you susceptible to fraudulent activity. Whatever the case may be, if you make passwords for each account unique, you are less likely to have all of your accounts compromised at once.


But it is hard to remember all those unique passwords you say? That is ok, you don't have to. This is where a password manager comes in to play. Coming soon: The University has signed an agreement to use the password manager called LastPass. This password manager can not only keep track of all your passwords in a hardened encrypted format, but also allow you to use them across your computers and peripherals. You can even take it with you when you leave the institution (the license gets transferred into a personal license which is free to use).

**Resolution #2 Plan for Upgrades, Updates, System/Software Reassessment**

Sometimes we forget that even our **software, systems and services** need to go through a review. We need to determine if the software we have been using requires an overhaul due to being outdated/obsolete. Not just in terms of having to do software updates but in terms of reviewing the technology age, functionality, cost, and complexity.



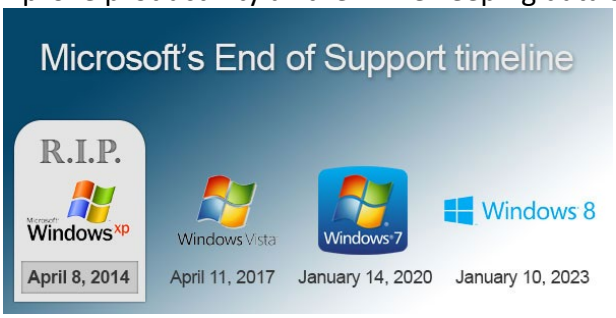




This is especially true when it comes to software, systems or services that have reached a vendor "End of Support Life" where security updates, enhancements, or bug fixes are no longer being provided. The upside to doing a review is that sometimes there are ease of use technology features that we can take advantage of. Some questions to ask:

- Is the software, system, or service obsolete? Can it run on the newest operating systems?
- Is it costing too much money to maintain vs getting a new one?
- Does it still meet the business requirements?
- Are workarounds currently in place to get software, systems, or services to function?
- Do they have complex and excessive configurations that can't be replicated or backed up?

- Are you doing manual work where a newer system can automate a task?

Doing a review can help give a clear and comprehensive overview of the implemented systems, software, services, and improve productivity all the while keeping data secure.




**Resolution #3 Review your accounting practices/policies**

Sometimes we forget to remove accounts we no longer use on services we apply for or systems/applications we have administrative access to. Those accounts likely contain personal data, identity details, and in some cases credit card numbers. By not doing anything to clean those up, in an age where data breaches are becoming all too common, we open ourselves up to future attacks. Here are some online resources to help you do some clean up:

- Online Search site:

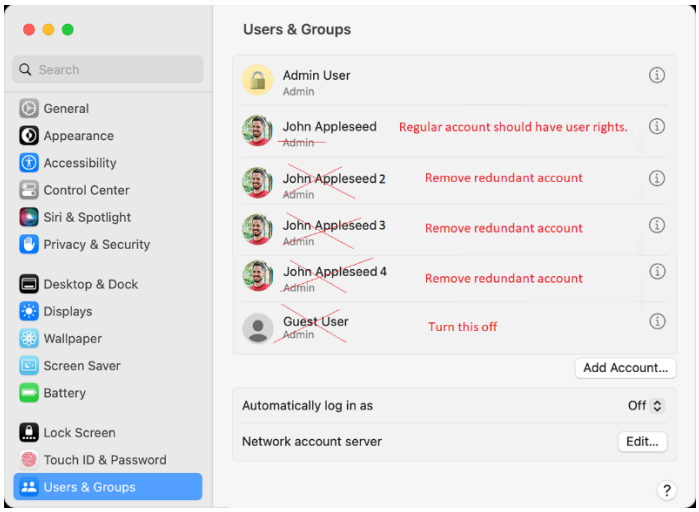
You can do a search on the following website to help review your e-mail address and find out where, when, and how it has been part of a security breach.
https://haveibeenpwned.com/
If you are still using a service that has experienced a breach, make sure you change your password. In some cases, you can also update your e-mail address to have an extension so that you can identify where an e-mail may be coming from. For example: If the service allows for special characters in an e-mail address, and you have a google account, google allows you to add a + sign at the end of your username in your email address. So instead of signing up for services with <username>@gmail.com you can sign up using an addition symbol + as follows: <username>+<signupservicename>@gmail.com. This allows you to identify the "From" origin most of the time.

- E-mail checks:

As for services you no longer use or have signed up for (and like a lot of us probably forgot about) you can search your e-mail for keywords such as "Welcome", "Your Account", and "verify" to review typical e-mail that introduce you to services. Most companies when sent an e-mail requesting that your information be deleted will honor your request unless a privacy policy or stipulation was added as part of the signup.

- System clean up:

For those devices, systems and applications brought from home or not administered by the BSD. It is important to review the accounts that exist on your system and do some clean up.




Not cleaning up accounts, and creating generic accounts creates access and accountability issues.

**Resolution #4 Review application configuration settings/privacy settings.**

We have mentioned this one before in one of our previous newsletters. Sometimes we use applications and forget to lockdown/configure/spend time setting the security/privacy settings. A great website for reviewing those privacy settings can be found here: https://staysafeonline.org/resources/manage-your-privacy-settings/


Feel free to contact us with any questions or topic suggestions at security@bsd.uchicago.edu. We want to hear from you!

Have a Happy and Festive Holiday Break!

-BSD Information Security Office