Apply Updates
Set your software to auto-update. Install updates and restart if needed.

Click Wisely
Click only links and files that are expected, and only from people you trust.

Use Strong Passwords
Create passwords that are unique and hard to guess. Use 2-step verification where available.

Know Your Data
Follow the policy to secure sensitive data. If you don’t need it, delete it.

You help keep Harvard secure.

For security tips and information, visit our website: security.harvard.edu.

To get assistance or report an incident, contact the Service Desk: 617-495-7777 or ithelp@harvard.edu.


security.harvard.edu
Click Wisely

Apply Updates

Use Strong Passwords

Know Your Data

There is a simple reason so many cyber attacks begin with phishing—it works. When you receive an unexpected message urging you to act immediately, it’s time to slow down and think. Using good judgment now will prevent headaches later.

Phishing Defined
Phishing is an email scam tricking you to click a link or open an attachment. The request may seem like it comes from a person or group you know, and it may seem urgent. If you fall for the scam, you might install malware or expose your password.

When to Report
Phishing is very common. You may see phishing emails that masquerade as notices from major banks or government entities. If you see a phishing email that looks like it came from Harvard—using our logos and branding—please contact the help desk immediately.

Most cyber criminals exploit known bugs, for which fixes have already been released. When you apply your updates and restart your system, you are fixing those bugs. Updating your software is a simple way to keep your device protected from most attacks.

Stop the Malware
Malware on your computer can steal your passwords or hold your data for ransom. When you install updates regularly, the malware fails. So, the next time your system prompts you to install updates and restart—don’t delay!

End of the Road
If the updates stop coming, does that mean there are no more bugs? No! Manufacturers eventually stop supporting their older products as new ones replace them. If you’re using outdated products—such as iPhone 4 or Windows XP—plan to upgrade as soon as you can.

When you use unique passwords, one lost password doesn’t compromise all of your accounts. Avoid using personal information, such as birthdays or pet names. Longer passwords are stronger passwords.

Step it Up
When you enable 2-step verification, any time you use your account on a new device, an authorization code will come to your phone. Without the code, a password thief cannot take control of your account. Use it with Google, Facebook, and more. It is the single strongest way to protect your account.

How to Manage
You have dozens of accounts, and that means you need dozens of strong passwords. Thankfully, there are applications to help you keep track of them. A password manager will help you create, use, and store passwords easily. Download one now, or ask your IT security team for help choosing one.

Most cyber criminals exploit known bugs, for which fixes have already been released. When you apply your updates and restart your system, you are fixing those bugs. Updating your software is a simple way to keep your device protected from most attacks.

Stop the Malware
Malware on your computer can steal your passwords or hold your data for ransom. When you install updates regularly, the malware fails. So, the next time your system prompts you to install updates and restart—don’t delay!

End of the Road
If the updates stop coming, does that mean there are no more bugs? No! Manufacturers eventually stop supporting their older products as new ones replace them. If you’re using outdated products—such as iPhone 4 or Windows XP—plan to upgrade as soon as you can.

When you know the data you store on your devices and services, you can then secure or delete it appropriately. The information security policy will show you the right way to identify, secure, and dispose of sensitive information.

Digging through Data
Not sure if you have private data on your devices? There are applications to help you check. Call the help desk to find out what software is available and how to use it.

Share with Care
Do you store and share data in the cloud? Some services don’t have the proper security to protect sensitive data. Your IT security team can point you toward services that are more secure for sensitive information.

When you know the data you store on your devices and services, you can then secure or delete it appropriately. The information security policy will show you the right way to identify, secure, and dispose of sensitive information.

Digging through Data
Not sure if you have private data on your devices? There are applications to help you check. Call the help desk to find out what software is available and how to use it.

Share with Care
Do you store and share data in the cloud? Some services don’t have the proper security to protect sensitive data. Your IT security team can point you toward services that are more secure for sensitive information.

When you know the data you store on your devices and services, you can then secure or delete it appropriately. The information security policy will show you the right way to identify, secure, and dispose of sensitive information.

Digging through Data
Not sure if you have private data on your devices? There are applications to help you check. Call the help desk to find out what software is available and how to use it.

Share with Care
Do you store and share data in the cloud? Some services don’t have the proper security to protect sensitive data. Your IT security team can point you toward services that are more secure for sensitive information.