We face many threats online today, but have limited time and attention to address them. Performing a risk assessment will aid you in prioritizing your efforts at protection. The threat model for someone worried about the NSA spying on them is very different from someone worried about identity theft or corporations spying on them to sell their information to advertisers.

Every account you have should be evaluated on the above table. The darker the red, the more vulnerable you are. For each service ask yourself, how easy is this to compromised? and how big a deal is it if it is? For example, email accounts are frequently compromised (easy to do) and have a big impact because most of your accounts link back to your email. So securing your email should be a high priority.

After you have prioritized your accounts you need to ask what can be done to proactively protect your account? For example, with email you can enable two factor authentication, use a strong password, and educate yourself about phishing.

Finally, think about what can be done to limit the damage if an account is compromised. For instance, using different passwords for each account will keep one compromise from compromising everything.
Malware is a generic term for MALicious softWARE. There are many different terms for malware. Here are a few terms that you may hear:

Virus - self replicating program that can be spread from one computer to another

Adware - advertising software that installs itself onto your computer

Spyware - software designed to send information about you to a company

Scareware - a program that causes threatening messages to pop up designed to get you to buy a product

Ransomware - software that encrypts your files and threatens to delete them unless you pay a ransom

Backdoor – software which allows remote access to your device, allowing an attacker to control it.

Bloatware – extra software installed by manufacturers It isn’t necessarily malicious, but sometimes can be.
Phishing and Spear Phishing

Phishing is a scam using email to get you to click on a malicious link, open an attachment, or provide information.

For example, an attacker may send an email that appears to be from your bank that contains a link. Clicking the link will take you to a site that appears to be your bank, but isn't. When you enter your password and account number, you have just given your bank information to an attacker.

Spear phishing is like normal phishing, but it uses personal information about you to gain your trust. This information could come from another hacked site, public records, or a data breach of a company that had information about you.
Avoiding Phishing

- Identify phishing emails
- Never click on links in emails
- Be suspicious of email attachments
- When in doubt contact the company that an email claims to be from

The most important thing that you can do to avoid being a victim of a phishing scam are learn to identify phishing emails. Here are some things to look for:

- Emails asking for personal information - These will often appear to be from organizations that you do business with. They may say that they need to verify your information for security purposes or use other scary language.
- Emails with links to click on - Scammers often will include links that say they go to one place but actually go to another. For example if you click on the following link www.google.com you will find it doesn't take you where you expect it to. Scammers use this to direct you to their websites to harvest any information (username, password, account number, etc) that they can get you to type in.
- Emails that contain attachments are VERY dangerous - Attachments on emails can contain all kinds of malware and viruses. Simply opening the file can be enough to infect your system. This is the number one source of infection for a new type of virus called cryptolocker which encrypts all your files and threatens to delete them if you don't pay them a ransom.
Phishing Response

- Do Not click on any links
- Forward the email to spam@uce.gov
- Contact the bank or company that the email claims to be from to alert them
- Do Not respond to the email

So what can you do if you think an email is phishy?
1) Never give out personal information in response to an email. If your bank emails you and says that they need to verify your information, call your bank to be sure that the email is legitimate, or go directly to their website using a web browser. Do not respond to the email at all.
2) If an email asks you to click on a link, do not do it. Even if it is from someone that you know. It is possible that their email has been compromised and scammers are using it to infect other people. If you want to visit the link, go to a web browser and navigate to the site. This ensures that you are going to the site that you think you are.
3) Do not download an open attachments unless they are from someone that you know and you are expecting the email. Even then make sure that you run a virus scan on the file before opening it.
4) Forward any phishing emails to spam@uce.gov to report it. Also, contact whatever organization the email claims to be from to alert them of the scam. This will allow them to let others know about the scam.
5) After this, delete the email. Do not respond to it.

If you follow these steps, you should be much better protected against phishing scams. Keep in mind that these emails can be extremely convincing.
Do your updates! As software companies learn about vulnerabilities, they send out fixes. By not doing updates, you are making an attackers job easy by letting them use known exploits against you. Any software that is on your computer needs to be kept up to date. For example:

Your operating system.

For a Mac, you can access updates through the app store. For more information go to https://support.apple.com/en-us/HT201541

Flash - https://helpx.adobe.com/flash-player.html

Antivirus - If your antivirus isn't up to date, it can't find all of the viruses out there.

Web browsers - These directly interact with the internet and must be kept up to date.

This isn't a complete list by any means. Every piece of software on your computer needs to be kept up to date or it may turn into an exploitable vulnerability. By using a applications auto-update features, you get the protection without the effort.
Windows Updates

Start button → Control Panel → Systems and Security → Windows Updates
If your computer is connected to the internet at all, you need antivirus. Antivirus programs aren't magic pills that eliminate any threat, but they are a powerful tool for ensuring your safety. When looking at Antivirus programs consider the following factors:

Features - does it provide features like scanning all downloads? What about email attachments?
Ease of use - are you comfortable with the design and do you find it easy to navigate?
System resources - especially for older computers, antivirus programs can be resource hogs. Your computer only has so much processing power and memory available. If your antivirus program is taking it all, it can really impact your computers speed.
Cost - Antivirus programs range from free to hundereds of dollars. Choose one that fits your budget, but don't overlook free offering just because they are free. Sometimes they perform better than expensive alternatives.

To help pick out an anti-virus program, check out the following sites:

http://www.av-comparitives.org/
https://www.av-test.org

These organizations test antivirus programs and rank them based on their performance and are extremely helpful for finding the best product for you.
Backups protect important information against malicious acts (such as ransomware), accidents (hard drive dies or computer is lost), and disasters (home burns down). The 3-2-1 ensures that your backups are protected against all of these. Backup anything that you can’t be easily replaced on your computer.

3 copies of your data ensures redundancy. A virus or hardware failure won’t wipe out your data. 2 different types of media means you aren’t storing both copies on the same hard drive. Having one copy on your computer and one copy on an external hard drive or thumb drive means that your computer dying or getting stolen won’t mean you lose everything. 1 copy offsite protects against disasters such as your house burning down or getting flooded. One copy being physically separated means you have a safe copy regardless. Cloud backups are a popular way to get an offsite backup.

Compare Cloud backup software at:
https://en.wikipedia.org/wiki/Comparison_of_online_backup_services
Passwords

A Long password is a strong password

- **Password 1 “%Ab3$9”**
  - 6 Characters, uses upper case (26), lower case (26), numbers (10) and special characters (36)
  - Possibility of guessing is 1 in $98^6$ or 885,842,380,864
- **Password 2 “Correct Horse Battery Staple”**
  - 28 Characters. Uses upper case (26), lower case (26) and Spaces (1)
  - Possibility of guessing is 1 in $53^{28}$ or 1 in $190,425,168,600,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000$, 0

Passwords are absolutely essential to good computer security. Using weak passwords and reusing passwords are some of the most common mistakes that people make. Unfortunately, these mistakes make any potential breach, such as hacking someone's email, much more serious. If you reuse passwords, and there is a VERY good chance you do, then getting your password for one thing often means they have your password for a lot of other things too.

Here are two points to remember about passwords:
1) Long passwords are strong passwords. Adding length to a password makes it much harder to guess than adding complexity. The only caveat here is that choosing a very long dictionary word doesn't help at all. Hackers have files with millions of words and variations on words that their computers can try very quickly to crack a password.
2) You must use a different password for each site. A credential stuffing attack is where a hacker takes a compromised account and sends those credentials to a bunch of websites (the top 10,000 websites on the internet for example) to see if they work. This allows attackers to multiply to effects of a single compromise and requires very little effort on their part.
Safely Storing Passwords

- Write it down
- Use a password vault
- Use two factor authentication

The reason that people reuse passwords is that there are simply so many passwords required in modern daily life. It is completely impractical to remember them all.

Here are some strategies to deal with this complexity.

1) Write down passwords. It is hard to hack a note book. This isn’t the most secure way of dealing with passwords, but it is far far better than just reusing passwords. It is hard to keep updated, and does nothing to help you come up with good passwords though.

2) Use a password vault – This software will generate and store passwords for you. This lets you use strong unique passwords for every site. Popular password vaults are:
   1) Keepass – free and open source. Stores passwords locally. [https://keepass.info/](https://keepass.info/)

3) Use two factor authentication – Uses something you know (your password) along with something you have (normally a cell phone) to add an extra layer of security.