Sources:

https://www.kaspersky.com/resource-center/threats/what-is-cybercrime

**What is cybercrime?**

Cybercrime is any crime that takes place online or primarily online. Cybercriminals often commit crimes by targeting computer networks or devices.

How to protect yourself against cybercrime?

1. **Use strong passwords** – do not repeat passwords on different sites and change your passwords regularly. Make them complex or hard to guess. This can protect against hacking usually achieved by technologies that are capable of a brute force attack.
2. **Keep your software updated** – cybercriminals frequently exploit known weaknesses or flaws in your software to gain access. Software developers usually provide updates that patches these flaws, thus avoiding further damage by means of eradicating the possible source.
3. **Manage your social media settings** – keep your information to yourself. Public profiles such as Facebook, wherein your information might be viewed publicly is actually a frightening concept. Cybercriminals may do a lot than just impersonating your profile to cause maliciousness.
4. **Strengthen your home network** – it is a good idea to start with a virtual private network (VPN). A VPN will encrypt all of your packets until it arrives at its destination. If cybercriminals manages to hack your network lines, the best that they can see will be encrypted data. Thus, rendering attacks such as packet sniffing useless.
5. **Know what to do if you become a victim** – report to your local police if activities about cybercrime had been discovered. Even if it is minor, just report it, this can help the authority to innovate and be better prepared when it comes to preventing cybercriminals from taking advantage of other people.

**Examples of Cybercrime**

Here are some infamous examples of different types of cybercrime attack used by cybercriminals:

1. **Malware attacks** – a computer compromised by malware could be used to by cybercriminals for several purposes such as ransom attacks, stealing confidential data, damaging data, spying etc.

A famous example of a malware attack was the WannaCry ransomware attack, a global cybercrime committed in May 2017. WannaCry is a type of ransomware, malware used to extort money by holding the victim’s data or device to ransom. The ransomware targeted a vulnerability in computers running Microsoft Windows.

When the WannaCry ransomware attack hit, 230,000 computers were affected across 150 countries. Users were locked out of their files and sent a message demanding that they pay a Bitcoin ransom to regain access.

Worldwide, the WannaCry cybercrime is estimated to have caused $4 billion in financial losses.

1. **Phishing** - A phishing campaign is when spam emails, or other forms of communication, are sent with the intention of tricking recipients into doing something that undermines their security. Phishing campaign messages may contain infected attachments or links to malicious sites, or they may ask the receiver to respond with confidential information.

A famous example of a phishing scam took place during the World Cup in 2018. According to our report, 2018 Fraud World Cup, the World Cup phishing scam involved emails that were sent to football fans. These spam emails tried to entice fans with fake free trips to where the World Cup was being hosted. People who opened and clicked on the links contained in these emails had their personal data stolen.

1. **Distributed DoS attacks** - Distributed DoS attacks (DDoS) are a type of cybercrime attack that cybercriminals use to bring down a system or network. Sometimes connected IoT (Internet of Things) devices are used to launch DDoS attacks.

A DDoS attack overwhelms a system by using one of the standard communication protocols it uses to spam the system with connection requests. Cybercriminals who are carrying out cyberextortion may use the threat of a DDoS attack to demand money. Alternatively, a DDoS may be used as a distraction tactic while another type of cybercrime takes place.

A famous example of this type of attack is the 2017 DDoS attack on the UK National Lottery website. This brought the lottery’s website and mobile app offline, preventing UK citizens from playing. The reason behind the attack remains unknown, however, it is suspected that the attack was an attempt to blackmail the National Lottery.

**Penetration Testing (Pentest)**

It simulates an attack on a system to evaluate its security. As a pentester, the job is to assess and identify weaknesses of a computer system.

Weaknesses in regards of network, software, social engineering etc.

Penetration testing requires skills that combines technical and non-technical skills. But the technical one is obviously the hardest part wherein deeper knowledge about the concepts of computer science is a must.

**Programming in the World of Cyber Security**

The highlight for today would of course, the importance of programming in cybersecurity. Though it may be true that penetration testing is usually done using a tool, but if we were to think about it, those tools are also developed by programmers.

As a programmer, you can formulate better ideas if what are the possible ins and outs of a cybercriminal by thinking like a cybercriminal. Hacking revolves around the weaknesses of systems wherein cybercriminals usually develop their own tools/devices to hack into the system.

**Best Programming language to learn for Penetration Testing as of 2023**

1. Python
2. Bash
3. Ruby
4. Perl
5. C/C++

Overall, Python is a good language to start with as it is widely used and has a large support from its community thus, having vast resources for penetration testing needs. However, do remember that programming is just one aspect of penetration testing, a good penetration tester should have broad range of technical and non-technical skills.