Hacking

Introduction

Technology is being developed day after day with a great speed, if you can't adapt with this development you'll be isolated from the world, or it could affect your career or the opportunities that you can get. also, computer science plays an important role in our lives and this role is increasing very rapidly, so in this report we'll introduce to you just a branch from the tree of computer science.

The more you know about hacking, the more you should beware of it. Therefore, in this report, we will not only focus on the definition of hacking, its types, methods, and tools of hackers, but also we will focus on its harm and show you some of the accidents or disasters caused by hacking.

Objectives

1. **Understand what the meaning of Hacking.**
2. **Present a simple abstract about technology field.**
3. **Limit the use of programming skills in a way that may harm people.**
4. **Make professional programmers turn to useful areas.**

1. Understanding what the meaning of hacking

Today you can't be isolated from the world because the concept of distances between people has diminished in the past twenty years .thus anyone who uses a computer connected to the Internet is susceptible to be hacked . so that , we present to you some information that may be interest you in this field .

Basically , Hacking is searching for any weakness in your computer system or networks to exploit this weakness to be able to access, and for example: Using password cracking algorithm to gain access to a system . And the person who does it is called "Hacker"

1.1. The hacker and his types

Hacker is a witty skilled programmer who can handle codes easily and quickly. this guy is not always the same guy who might be in your imagination. There are three basic types of hackers (whit, grey or black hat hackers). this terminology originates in the Western Popular American culture, in which refers to cowboys.

Generally, a white hat hacker hacks under good intentions with permission, a grey hat hacker who hacks with good intentions without permission and a black hat hacker has malicious intent.

1.1.1. White hat hacker

the term "white hat" means an ethical computer hackers they are a skilled computer programmers , who specializes in penetration testing , unlike black hat

Basically, the white hat hacker works against the black hat hacker as the black hat tries to steal your information through the techniques he uses like :

- Trojans
- Viruses
- Social Engineering
- Worms
- Network Enumeration
- SQL Injection
- Denial of Service (DoS)
- Brute Force Hacking

The ethical computer hacker works to stop that .

One of the first times that it shows the usefulness of a white hat hacker or the so-called ethical hacker was a "security evaluation" conducted by the United States Air Force The evaluation found that the system used has a vulnerability that can be accessed and the matter was very dangerous and would lead to serious consequences , They performed tests that might damage its integrity, but it still so useful especially for organizations that have to be very secretive.

so the white hat hacker hacks under good intentions with permission as mentioned before.

There are many jobs in this field that could interest you in your career and to be a white hat hacker ,achieving the Certified Ethical Hacker (CEH) certification from the EC-Council is one recommended starting point.

The median salary of an ethical hacker is almost $80,000, according to PayScale, and the top range can climb to well over $100,000. On the consulting side, the EC-Council states that CEH professionals can expect to be paid $15,000 to $45,000 per contract or short-term assignment.

They are also called "sneakers", red teams, or tiger teams.

1.1.2. Grey hat hacker

The grey hat hackers are in between white and black hackers who break into computer system or network but not with the aim of sabotaging your data as black hat hackers do. They are computer security experts who may sometimes violate laws or ethical standards bun not have a malicious intent.

You should know that “grey hat hacker” is taken from "white hat" and "black hat" hackers. For example, when the grey hat hacker discovers vulnerability, they will neither illegally exploit it, nor tell others how to do so.

Also they have their own method of discovering vulnerability. They generally have the skills and intent of the white hat but will break into any system or network without permission.

The grey hat hackers break into any system or network without permission and when they discover vulnerability, they offer to repair it for a small fee.

And for clarification …

There are many grey hat hackers. There are many names and many incidents as well. Like the one that happened in April 2000. The hackers’ name was "{}" and "Hard beat". they gained access to Apache.org. but they alerted the crew instead of damage the data.

In June 2010 ,Goats Security exposed a flaw in AT&T security , they revealed it to the media soon after alerting AT&T

1.1.3. Black hat hacker

Black hat hackers are a group of criminals who aim to steal our data for various reasons such as sabotaging it, changing it, or making it useless through break into secure networks they're the example that appears in the mind of ordinary person when you say " hacker" .It has involved until it has become a profitable field . Not just out of curiosity

Some of non-skilled hackers (script kiddies) who gain access to computer system using already made tools were trained to hack just for quick profit .

But the upper echelon of Black Hats tends to be skilled hackers who work for sophisticated criminal organizations and these organizations are just like any legitimate businesses. they provide collaboration tools for their workers and offer service agreements to customers .

So you cannot imagine how much damage these organizations do in the world and to governments especially it is extremely difficult to stop.

1.2. Techniques for hacking

The professional hacker has several methods and techniques for hacking and those are 5 most common websites hacking techniques you should know:

1. **Phishing**
   In his technique, the hacker repeats a specific website with the aim of stealing money or personal information. When the user uses that website and puts his personal information on it, the hacker steals it like a password or credit card details.

2. **Viruses and malicious code**
   Hackers can enter almost into any website and leave malware in its' database or insert code into the website's files. There is a big variety of viruses, and each may impact the infected site in different way.

3. **UI Redress**
   we can say that This technique is similar to phishing. But in this technique, a hacker creates a fake hidden user interface. when the user clicks the button, he will find himself on an unfamiliar website, with an inappropriate content

4. **Cookie Theft**
   in this case , the hacker can steal a lot of important information like browsing history, usernames and passwords which browser's cookies contain it .that data can also contain other important information like logins and password to your website's administrator's panel

5. **Denial of Service (DoS\DDoS)**
   in this technique, the hacker uses bots to interrupt or crash the

server. bots would send requests to the website, therefore, the server would crash because it unable to process all of the received requests. the hacker can crash the server in a relatively small amount of time and this makes it more dangerous

1.3. Hacking tools

Below are some of the most popular penetration testing tools that may help through the first steps of a security investigation. There is some of the classic tools that seem to have been around forever and some new tools that might not be familiar.

1. John the Ripper

John the Ripper is considered one of the most popular password crackers. It's also one of the best security tools available to test password strength in any OS, or for auditing one remotely.

This password cracker is able to automatically detect the encryption used in any password, and will change its password test algorithm, this is why it is one of the most successful password cracking tools ever.

This hacking utility uses brute force technology to decipher passwords and algorithms such as:

- DES, MD5, Blowfish
- Kerberos AFS

- Hash LM (Lan Manager), the system used in Windows NT / 2000 / XP / 2003
- MD4, LDAP, MySQL (using third-party modules)

Another bonus is that it is open source, multi-platform and available for Mac OS, Linux, Windows and Android.

2. Metasploit

Metasploit is one of the open source cyber-security projects that makes InfoSec professionals able to use different penetration testing tools to discover remote software vulnerabilities. It also works as an exploit module development platform.

One of the most known results of this project is the Metasploit Framework, which is written in a language called Ruby, which help you to develop, test and execute exploits easily. The framework includes a group of security utilities that can:

- Evade detection\security systems.
- Run security vulnerability scans and tests.
- Do remote attacks.

Metasploit provide three unique versions of their framework:

- Professional: better for penetration testing and IT security teams.
- Community: used by small companies and InfoSec students.
- Framework: the best for app developers and security researchers.

Supported platforms include:

- Mac OS X.
- Linux.
- Windows.

3. SQLmap

SQLmap is a cyber-security tool written in a language called Python that aids security researchers to launch SQL code injection tests against remote hosts.

With SQLmap you can stop and test a variety of types of SQL-based weaknesses to strengthen your apps and servers, or to report vulnerabilities to different companies.

Its SQL injection techniques include:

- UNION query-based
- time-based blind
- Boolean-based blind
- error-based
- stacked queries
- out-of-band

Main features:

- Multiple database server support: Oracle, PostgreSQL, MySQL and MSSQL, MS Access, DB2 or Informix.
- Automatic code injection capabilities
- Password hash recognition
- Dictionary-based password cracking
- Get password hashes
- View user privileges and databases
- Database user privilege escalation
- Dump table information
- Executes remote SQL SELECTS

Summary

Software companies reap the most benefits from the rise of automated ethical hacking tools and penetration testing utilities, giving them more ways to increase system security every day.

Automated tools are changing the way hacking is evolving, making ethical penetration testing easier, faster and more reliable than ever. Penetration testing and reporting activities now play a crucial role in the process of identifying security flaws in remote or local software — enabling company owners to quickly prevent vulnerabilities from running wild all over the Internet.

1.4. Some forms of hacking

Similarly, when a criminal is trying to hack an organization, they won't re-invent the wheel unless they absolutely have to: They'll draw upon common types of hacking techniques that are sure to be effective and efficient, like **malware, phishing, or cross-site scripting** (**XSS**). If you are trying to make sense of the latest data threat headline in the news or working on an incident in your own organization, it helps to understand the different attacks a malicious code might try to cause harm.

Here’s some of the most common and most popular types of attacks known to hackers.

Malware

Malware are various kinds of harmful code, viruses and ransomware for example. When a malware is in your computer, it can cause all sorts of chaos, it can take control of your machine, and browse your actions and keystrokes, and send all sorts of private data from your computer or network to the attacker's base.

Phishing

A phishing attack is when an attacker sends you an email that looks from someone you trust, like your boss or a company you do business with. The email will seem legitimate, and it might be urgent (example: fraudulent

activity has been detected on your account). In the email, there might be a file to open or a link to go through. After opening the attachment, you'll install malware in your computer. If you click the link, it may send you to a legitimate-looking website that asks for you to log in to access a confidential file, but in reality the website is actually a trap used to get hold of your credentials when you try to log in.

SQL Injection Attack

An SQL injection attack happens by exploiting any one of the known SQL weaknesses that helps the SQL server to run bad code. For instance, if a SQL server is weak against an injection attack, it may be possible for an attacker to go to a website's search box and type in code that would make the site's SQL server to delete all of its stored usernames and passwords for the site.

1.4.1. Cracking vs. Hacking

What is a hacker?

A hacker is a person who likes to have a deep understanding of the deep structures of a program, computers or computer networks. The term "hacker" is often wrongly used in a negative context, where 'cracker' should be the correct use of the term."

What is a cracker?

"A cracker is someone who tries to get into computer systems and applications without authorization. These people are often have bad intent, as opposed to hackers, and have many tools and utilities at their disposal for breaking into a system."

Crackers are also called "black hats." They look for backdoors in programs and systems, exploit those backdoors, and steal private information for use in a malicious way.

Differences between hackers and crackers

By now, many differences between hackers and crackers might seem obvious, but let's review their core differences:

Ethical difference

Hackers are the good guys, white hats who break into networks to discover loopholes, and to restore the security of corrupted networks to build a secure system. They never do it illegally and always inform their hiring organization or individual of their actions. They're a great weapon in the hunting down and catching of crackers. Crackers, however, will break into the same system for personal, financial or any other kind of gain without the knowledge or permission of the system owners, for the purpose of engaging in illegal activities.

Skill difference

Hackers possess the ability to create programs and software tools; they're skilled in multiple codes and languages and have advanced knowledge of various select computer languages. Crackers, on the other hand, don't need to possess a deep well of knowledge, save for the one on how to actually break a system, and we don't normally see them being skilled enough to create their own programs. Even with so few crackers skilled enough to create tools and software to help them exploit the weaknesses they discover, we should never ignore their threat.

1.4.2. Network Hacking

A network security breach occur when a network is entered by an unknown user or software. When they get inside the network, they can steal data, stop software or install malware.

A network security breach can be a disaster for any who work as an IT professional, or his clients, and even the biggest companies with high-level security measures have been a victim to a security threat.

Here are some of the results of any network security breach:

- Lost revenue
- Reputation damage
- Identity theft
- Theft of ideas, plans or other intellectual property
- Consumer mistrust
- Market share loss
- Shareholder wariness

International computer crimes

Most Common Types of Cybercrime Acts

1. Fraud

Fraud is a cybercrime that intends to deceive a person to gain private data or information. Fraud can be done by changing, deleting, taking, any information to get to an illegal goal.

2. Identity Theft

Identify theft is a specific form of fraud in which cybercriminals steal personal data, including passwords, data about the bank account, credit cards, debit cards, social security, and other sensitive information. Through identity theft, criminals can steal money. According to the BJS, more than 1.1 million Americans can be a victim by identity theft.

3. Ransomware

Ransomware is one of the most hurtful and dangerous malware-based crimes. It gets into your computer network and encrypts all files and information through key encryption. In 2016, over 638 million computer networks had been hit by ransomware. In 2017, over $5 billion is lost because of international ransomware.

2. present a simple abstract about technology field.

Technology is good because it simplifies the way we do things in our daily lives, however, if the technology is wrongly applied. It can be harmful in so many ways.

Technology is developed by humans, so we can use it to accomplish almost every task. It makes the impossible look possible.

2.1 The meaning of technology and examples.

Technology is a body of knowledge devoted to creating tools, processing actions and the extracting of materials.

We use technology accomplish various tasks in our daily lives. We can describe technology as products and processes used to simplify our daily lives. We use technology to extend our abilities, making people the most crucial part of any technological system.

Technology is also an application of science used to solve problems.

We apply technology in almost everything we do in our daily lives. We use technology at work, we use technology for communication, transportation, learning, manufacturing, securing data, scaling businesses and so much more.

Technology is human knowledge which involves tools, materials and system. The application of technology typically results in products If technology is well applied, it benefits humans, but the opposite is true, if used for malicious reasons.

Some examples of technology:

- *Tablets*
- *Laptops*
- *Robotics*
- *Digital cameras*

2.1.1 Technology plays an important role in every sphere of life.

Technology plays a major role in modern life that affects all the aspect of human activities. Therefore, our societies get a lot of benefits from modern technology. And we use technology to accomplish various tasks, so technology comes in different forms.

1- Communication Technology

This is a system that uses technical means to transmit information or data from one person to another or from one place to another.

Communication is a daily essential for all. It is used to convey ideas exchange information and express emotions. Human use communication

technology tools like phones, computers, emails and more.

2- Medical Technology

This is the type of technology which is used to extend and improve human life. Medical technology reduces patient 's pain and cares for an injury.

new ways of competing with well-established companies. To some extent, some business technologies can make a small company look like a big company, and this can help a small business gain position in a competitive And it is used to diagnose infections, treat diseases and to research diseases affecting humans, etc..

3- Information Technology

Information technology is a set of hardware and software tools used to store, transfer and process information. Information technology tools help in providing the right people with the right information at the right time. Like

banks use information technology to operate their entire businesses as well as serve their customers.

4- Entertainment Technology

This use of technology to create an entertainment experience.

Technology is used to create video games, to develop musical systems and so much more.

5- Business Technology

This is technology used to run a business and enhance various business operations.

Many businesses are using technology to scale its growth. Small business has used technology to create market.

2.1.2 Technology has revolutionised the field of education.

6- Education Technology

Education technology aims at improving a student performance by creating and managing various technological processes and resources.

Schools and university for example have so many facilities. devices, internet connections with high speed, projectors and smart boards.

Using these developed tools can help students in many ways.

First student can study and understand their subjects well when they use audio-visual technology.

Second, students may pass their exams online

Third they can access a lot of resources like libraries, websites and scientific paper online.

These facilities may help students master their subjects, save time and stay in touch with the new world.

2.2 *Technology will be required for computer programmer.*

The more the technology becomes; the more advanced and developed is the computer programming.

Nowadays, people can't live without programming, because programming helps us in every aspect of life.

We need different types of technology to practice our work as computer programmers.

People use technology in many different places; laboratories, schools, hospitals, companies and colleges.

In order to be a successful programmer, you need to master how to deal with different computer programs and be able to solve any problems that can get in the way of the process of programming

Computer programmers write,code the programs that tells computers what to do.

This is accomplished by converting the software program that designed by software engineers, into a series of insturctions a computer can follow.The job is multifaceted in that it entails creating ,adapting, modifying,troubleshooting and maintaining programs. Although having a bachelor's or master's degree is most often required for computer programming jops, those with related work experience may only need a certificate or associate's degree.

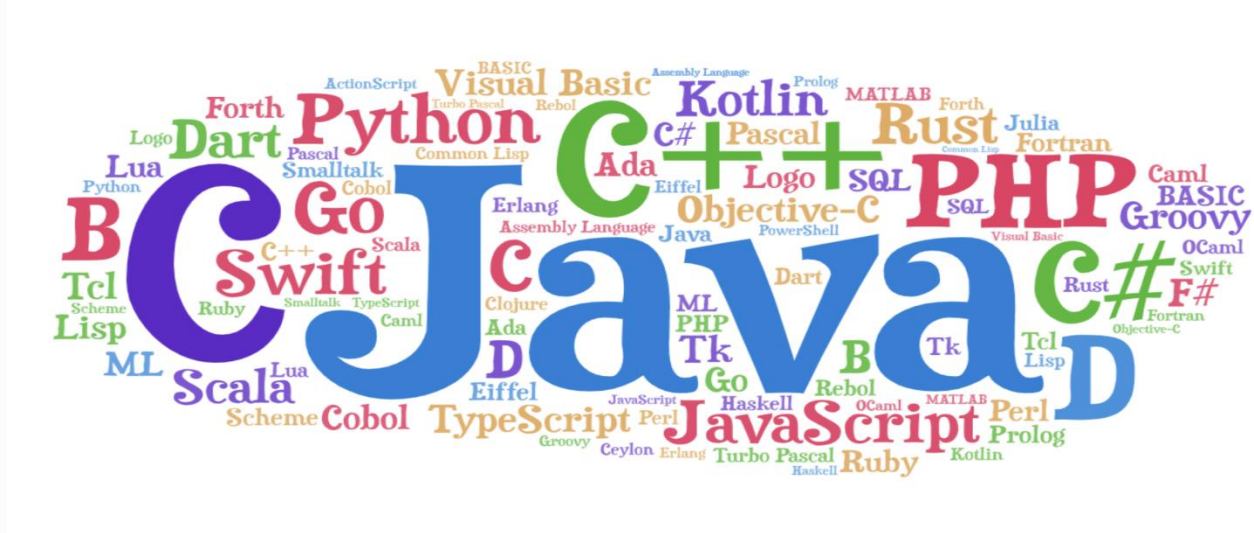
Depending on where they work,programming may also need to seek certification.

2.2.1 T*he difference between technology and language programming.*

I believe that there is a major different between technology and programming.

If I am a regular user not a programmer, I will use basics and simple applications and programs. But if I am to be dealt with as a computer programmer, I have to be able to deal with different types of language programming. As well as knowing how to deal with hardware. If you are interest in computer hardware and software but you aren't sure which career path to choose, you probably want to learn about information technology (IT)and computer science. Those two rewarding careers each require a slightly different set of skills, and they each appeal to a somewhat different type of person. An IT career involves installing, organizing and maintaining computer systems .as well as, designing and operating networks and databases.

Computer science is focused entirely on efficiently programming computers using mathematic algorithms.



2.2.2 *Technology is set of programmers to find a new way of solving current systems backlogs.*

Backlogs are accumulation of uncompleted work or matters needing to be dealt with.

In order to solve these backlogs or problems, we have to use technology that will help and ease the process of solving current systems backlogs.

Using technology, we can help backlogs in a creative and brilliant way that users can understand and deal with it easily.

HOW TO MAKE THE BACKLOGS LEARN?

Here are a few action items for improving your backlogs size.

1.Take The Product Owner Role Seriously.
2.Limits Design In Process.
3.Decide How To Manage The Backlogs.
4.Make Decions.
5.Work With An Aging Ideal Funnel.
6.Follow Your Own Rules.

3. Limit the use of programming skills in a way that may harm people.

- **Weakness points**

There are a lot of programs available online that search for vulnerabilities, detect errors, and protect from malware. Spending money is not necessary, and you can install an effective program that informs you of any errors or defects in your system.

For Example:

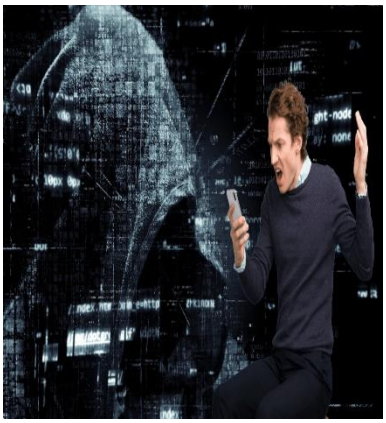
ESET NOD32, Avant, AVG, and Panda are some of the most popular and respected for next year

- **Encrypt your data yourself**

While backing up your data in case of an emergency is a must, first be sure to encrypt it yourself as a stronger approach to data protection. You can make your own data unreadable (thus unusable) to hackers, by encrypting the entire hard drive, a section of your hard drive, or a singular file by file process. This might sound excessive and maybe beyond your technical skills, but it's actually easier than it sounds.

There are plenty of free disk encryption programs available online that "work by forcing a user to provide the decryption password before the operating system loads." Or, you can opt for a pricey one to gain access to more advanced features.

3.1. Types of harm to people as a result of Programming (Hacking).



Becoming the victim of cyber crime can have long lasting effects on your life. One common technique scammers employ is phishing, sending false emails purporting to come from a bank or other financial instiution requesting personal information. If you hand over this information it can allow the criminal to access your bank and credit accounts as well as open new accounts and destory your credit rating this type of damage can take months or even year to fix this

The overall monetary losses from cyner crime can be immense. According to a 2012 report by symantec mora than 1.5 million people fall victim to some sort of cyber crime every day ranging from simple password theft to extensive monetary swindles with an average loss of $197 per victim this adds up to more than $110 billion dollars lost to cyber crime world wide every year as consumers get wise to traditional avenues of attack cyber criminals have developed new techniques involving mobile devices and social networks to keep their illicit gains flowing and the cyber crime of privacy has had major effects on the entertainmen music and software industrise claims of damages are hard to estimate and even harder to verify with estimates ranging widely from hundreds of millions to hundreds o billions of dollars per year.

3.1.1. Electronic Stealing

Cyber attacks with financial demands. A modern take on blackmail, this can affect organisations of all sizes as well as individuals. There are many variations for example hackers takeover a victim's computer and freeze it, they then offer to reinstate access after a ransom has been paid.

Attacks to prepetrate a direct fraud on a business. This type of attack usually involves the diversion of funds from their legitimate destination to a fraudster's account. Crimnals use tehniques such as phishing and vishing to tease out enough information to enable them to mount an attack . They the access email systems and send emails the look legitimate but aren't. A variation of this attack is invonice fraud when an email is received that looks like it is from a legitimate supplier and is advising of a change of bank account details unfortunately, the bank account details supplied are those of a fraudster

There are vulnerabilities are usually a result of a user surfing the internet on shady sites , or opening up intrigung emails with phishing links that should have been categorized as spam in the first place

3.1.2. Harassment of communition sites

Before social media , The theft included material things However now, someone can be bullied online anonymously. Today everyone knows what cyberbullying is, and most of us have seen what it can do to a person. And

since screens hide our faces, you can end up being a harmfull on social media and other websites without realizing it.

While social media made making friends easier , it also made it easier for predators to find victims. The anonymity that social networks provide can be used by the perpetrators to gain people's trust and then terrorize them in front of their peers.

These online attacks often leave deep mantal scars and even drive people tp suicide in some cases. You'll be surprised to find out that cyber attack affects on all people.

3.2. Steps to take to protect people from hacking.

Change your password. For Example, sites that retain your credit card information or other sensitive data like (health records, for instance).

Keep an eye on your financial statements and bills. If you do get word from a company that its security was breached, take warnings to change your password seriously, if you have not done so already.

Make your passwords as strong as possible. The longer the better Aim for at least 10 Characters. Try to mix letters (not whole words from the dictionary) and number, both in numeral from and spelled out, but having discrete passwords acts as a safeguard if one site has a security leak, you won't be handing over keys to all of your information. Another smart idea Change your most important passwords for your email, your bank or other financial institutions, and sites like PayPal every 6 to 12

months. To help you remember your passwords, you could use a free password management service.

Enable multi factor authentication. Some sites offer the option of taking another one or two steps beyond entering a password in order to access information a PIN number, say. when possible, give yourself this additional protection.

Make Online Purchases from Secure sites any you make a purchase online; you need to provide credit card or bank account information just what cyber criminals are most eager to get their hands on. Only supply this information to sites that provide secure, encrypted connections. As Boston University notes, you can identify secure sites by looking for an address that starts with https: (the S stands for secure) rather than simply http: They may also be marked by a padlock icon next to the address bar.

Be Careful What You Download A top goal of cybercriminals is to trick you into downloading malware programs or apps that carry malware or try to steal information. This malware can be disguised as an app: anything from a popular game to something that checks traffic or the weather. As World advises, don't download apps that look suspicious or come from a site you don't trust.

3.2.1. International rules that programmers (hackers) are going to not harm people

The cyber-crime of piracy has had major effects on the entertainment, music and software industries. Claims of damages are hard to estimate and even harder to verify, with estimates ranging widely from hundreds of millions to hundreds of billions of dollars per year. In response, copyright holders have lobbied for stricter laws against intellectual property theft, resulting in laws like the Digital Millennium Copyright Act. These laws allow copyright holders to target file sharers and sue them for large sums of money to counteract the financial damage of their activities online.

The Computer Fraud and Abuse Act (CFAA) is the leading federal anti-hacking legislation that prohibits unauthorized access to another's computer system. Although the law was originally meant to protect the computer systems of U.S. government entities and financial institutions, the scope of the Act expanded with amendments to include practically any computer in the country (including devices such as servers, desktops, laptops, cellphones, and tablets).

Although much of the focus is on federal laws, states have enacted hacking laws as well. While every state has computer crime laws, some states address hacking more specifically with laws that prohibit unauthorized access, computer trespass, and the use of viruses and malware. and Ransomware occurs when malware is installed on someone's computer, denying access to the computer unless a ransom is paid. Several states, including California, have laws that specifically criminalize ransomware.

4- Make professional programmers turn to useful areas:

The field of hacking is very dangerous and it depends on the person who use it so most of countries make a great protection system to protect its economic system so all programmers must use the hacking in useful way .

Professional programmers concentrate their efforts to help people and governments to protect themselves.

It is very strange if we say that hacking may be useful in sometimes:

A study prepared by Gabriel Weiman, an international terrorism expert at Harvard University, Weiman shows how terrorists use the Internet for their malicious purposes as they spread their ideas on the social network and they search for dangerous information such as places of nuclear installations and places of military bases.

Here comes the positive role of hacking where hackers can monitor terrorist networks and know how they think so they can get ahead of them.

4.1. Professional programmer is responsible for international programming systems:

Programming is not an easy job as programmers have a great responsibility; programmers are responsible for international programming system.

Since technology began to expand in the world Most countries began using it to record important data and use technology for secret missions, whether military or economic And since then it has been the responsibility of programmers to create these systems tightly and develop them every period in a way that is proportional to the enormous expansion of technology in a short period of time.

And the programmer's mission is not limited to establishing the system or creating a database and developing it every period only. More importantly, it is to secure this system and make sure that it is difficult to penetrate it due to disasters that may cause the collapse of the state’s economy or the penetration of its military system.

4.1.1. Names of the most famous programmers :

1-Bill Gates:

Bill Gates is an entrepreneur; investor and richest man in the world who founded Microsoft, one of the largest software companies in the world in 1975, Bill and Allen founded a software company called "Microsoft" that means microcomputer software.

2-Ada Lovelace:

She was a mathematics specialist and was working on a Charles Babbage computer.

3-Niklaus Wirth:

He designed some programming languages, including Pascal, and won the Turing Award for developing a series of innovative computer languages.

4-Linus Torvalds:

A Finnish software engineer, best known for having developed a kernel known as Linux. It was named after the Nobel Prize-winning physicist Linus Pauling.

5-Guido van Rossum:

He is the inventor of the most important programming language in this era and is the Python.

	JOB OPENINGS	AVG. SALAR
C	2,000	$102,000
C++	14,500	$102,000
C#	27,000	$92,000
COBOL	2,400	$87,000
Java	46,000	$102,000
Objective-C	5,100	$103,000
PHP	10,800	$92,000
Python	15,200	$102,000
R	2,500	$85,000
Ruby	8,100	$105,000
SQL	150,000+	$92,000
Swift	1,500	$111,000

*The programming has a close relationship to piracy, so if we research, we will find that the programmers 'salaries reach very huge numbers because the professionalization of this field is difficult, so the real programmer is the one who can secure his program or the system that it establishes and protect it from penetration.

4.1.2. Professional programmers create international systems networks:

International intelligence has a sensitive place in the country. It monitors publications and maintains important data related to countries, their economy and their military systems, so it is concerned with establishing a robust protection system to secure all this information.

So all international programmers make system for every important foundation in the country such as banks , markets, governmental foundations and military installations.

4.2. Small errors lead to disaster:

The work in the field of programming international systems is very sensitive and every part of it must be done very carefully because any error will have severe consequences.

4.2.1. Reasons that may lead to gaps in the system:

Many black hackers try to violate the privacy of governments and control this information to use in terrorist purposes or to collect money and blackmail governments.

One of the most common types of penetration is the penetration of banking systems to control the money in these banks by exploiting

loopholes in banking systems, or it may be betrayal by the founder of the banking system itself.

Some hackers may steal or penetrate a large company's system and blackmail this company to take money to give away the information they have.

4.2.2. Famous accidents occurred in many countries:

-shadow brokers:

Shadow brokers is a hacking operation that occurred on August 17 after Shadow brokers managed to breach the US National Security Agency (NSA) and they got weapons that included running programs that the United States used to disrupt the Iranian nuclear program and decided to sell their information for $ 580 million.

-Cabana cyber gang:

It is a process that took about two years. The hackers penetrated the systems of many banks in more than one country around the world. These countries were the United States of America, Russia, Switzerland and Japan, and they obtained from this process a billion dollars.

New References

1-Morse, S. (2019, January 10). The Negative Effects of Hackers. Retrieved from https://itstillworks.com/negative-effects-hackers-2867.html.

2-Zhukov a, A. (2018, May 16). 7 Negative Effects of Social Media on People and Users. Retrieved from https://www.makeuseof.com/tag/negative-effects-social-media/

3-Team, S. T. (2018, October 9). Security Trails: Top 15 Ethical Hacking Tools Used by InfoSec Professionals. Retrieved from https://securitytrails.com/blog/top-15-ethical-hacking-tools-used-by-infosec-professionals.

4-Hernandez, E. (2018, August 22). The 16 Most Common Types of Cybercrime Acts. Retrieved from https://www.voipshield.com/the-16-most-common-types-of-cybercrime-acts/.

5-Common Types of Cybersecurity Attacks and Hacking Techniques. (n.d.). Retrieved from https://www.rapid7.com/fundamentals/types-of-attacks/.