INTERNATIONAL CYBERCRIME – ISSUES OF FRAUD, THEFT, AND EXTORTION

Aliev Avazbek Ulugbek Ugli
Teacher at the Digital Technologies and Information Security of the Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan

https://doi.org/10.5281/zenodo.18077864

Abstract. *This article highlights the types of cybercrime, their functions, the psychological, physical, and economic harm they cause to individuals, their consequences, the economic and social context of public policy, digital criminals that infringe on societal rights and freedoms, as well as distinctions between fraud and extortion in criminal law, including their defining signs and elements.*

Keywords: *Black Market Trading, Cybercrime[1], Cyberterrorism[2], Cyber Extortion[3], Fraud[4], Malware[5], Phishing[6], Password Attacks[7], DDoS Attacks[8], Man-in-the-Middle[9], Drive-by Download[10], Malvertising[11], Rogue Software[12].*

Today, the global information space faces new threats related to cybercrime, which are growing and evolving every minute. Therefore, the issue of protection against attacks in the virtual world is one of the serious challenges confronting the international community.

Furthermore, humanity's adaptation and integration into the cyber world is also a contributing factor. It is fair to say that the more advanced the times become, the more unimaginable life is without the internet and electronics, and the more cybercrime increases, permeating our entire lives and gaining the ability to control any sphere.

According to estimates, over 500 million cyberattacks are carried out worldwide annually.

Every second, one in 14 people becomes a victim of a cyberattack. In developed countries such as the USA, Russia, England, India, Germany, and Belgium, 60-65% of crimes are committed via cyberattacks. In Uzbekistan, the number of such crimes has increased 8.3 times and currently constitutes nearly 5% of the total crime rate. Specifically, there are frequent crimes involving the misappropriation of funds from plastic cards through illegal banking and financial operations, data theft, malicious viruses and risk-based games, opening hidden backdoors into computers or mobile devices, turning them into zombies, threats related to religious ideology, and fraud in the online commerce sector.

The types of cybercrime are increasing and evolving year by year, examples include:

1. Drug trafficking
2. Cyberterrorism
3. Cyber extortion
4. Cryptocurrency circulation
5. Cyberattacks
6. Promotion of pornographic products
7. Advertising fraud
8. Black market trading

Cyberterrorism - The use of the internet to carry out acts of violence involving threats of loss of life or serious bodily injury in order to achieve political or ideological gains through intimidation or coercion. Actions that deliberately and widely disrupt computer networks, particularly personal computers connected to the internet, using tools such as computer viruses, computer worms, phishing, malicious software, hardware methods, and programming scripts can be a form of internet terrorism.

Cybercrime is a term that refers to criminal activity involving computers, networks, or the internet.

Common examples of cybercrime include:

1. Malware (Malicious Software)
2. Phishing
3. Password Attacks
4. DDoS Attacks
5. Man-in-the-Middle
6. Drive-by Download
7. Malvertising (Malicious Advertising)
8. Rogue Software

Malware – Viruses and programs that infiltrate electronic devices such as smartphones, computers, ATMs, and other devices to extract information from them and gain access (permission). Via email inboxes, downloads to computers, and access to the operating system, they can turn the device into a "**Zombie**," allowing the attacker to enter at any desired time to steal data, disable it, send information, or conduct extortion.

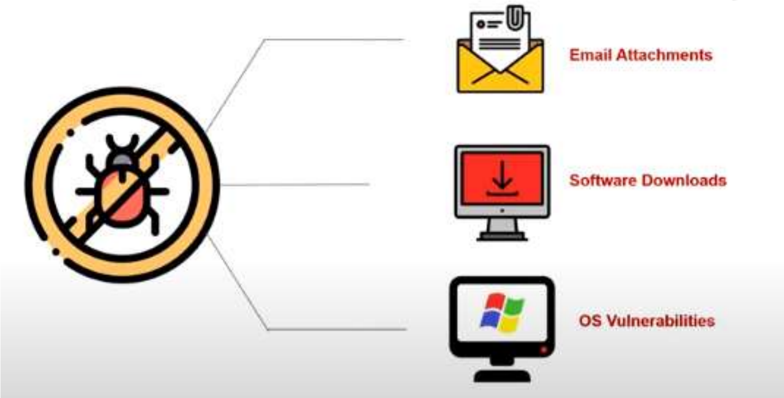
Types of Malware include:

- Computer virus
- Spyware
- Adware
- Worms
- Trojan Horse

Methods of Malware: Trojan Horse, Virus, Spyware, Adware, Worms

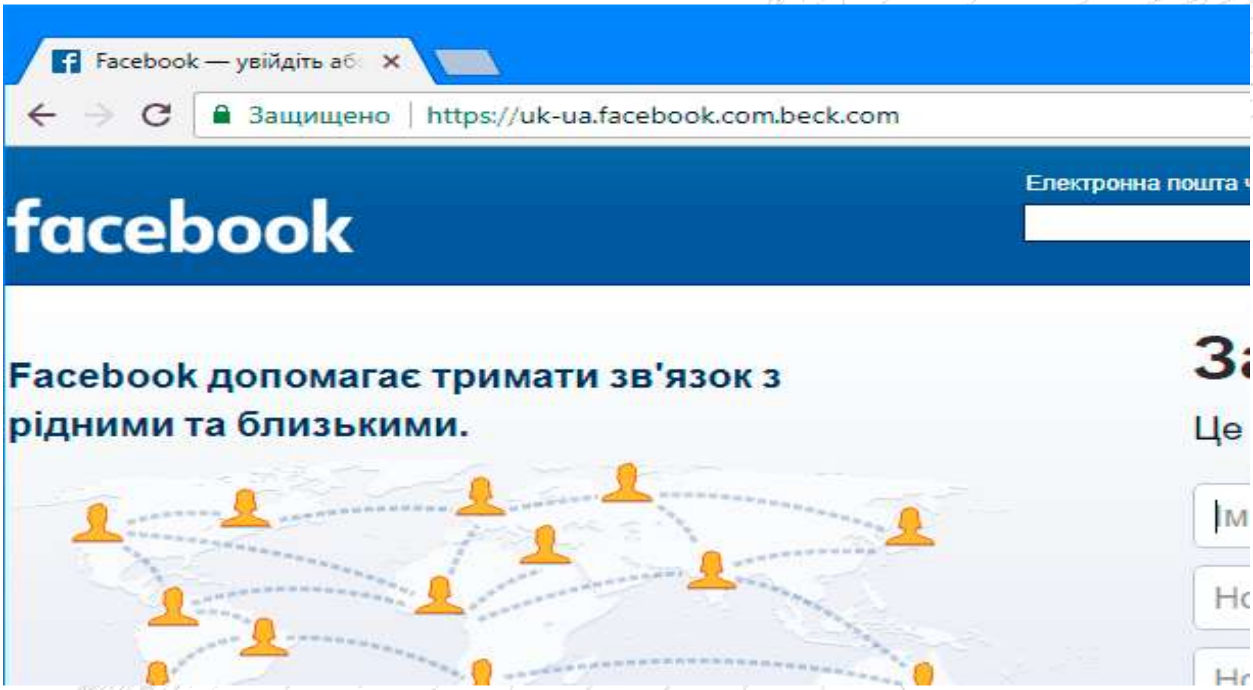
MALWARE
Computer Virus
Worms
Spyware
Trojan Horse
Adware
110110
010101

Ways malware gets connected:
Via email.
Through software storage.
Connects via the operating system



Phishing – Derived from "Fishing," it involves sending a person a link via websites or programs. When the person opens it and enters their personal information, the attacker collects the person's data. It is a method designed to steal login credentials, passwords, website data, email accounts, and bank card information for misuse.

On a state level, it involves obtaining information from high-ranking state officials, withdrawing money from their accounts, or gathering compromising information against an individual, then offering material valuables or services in exchange for the official's silence.



Facebook допомагає тримати зв'язок з рідними та близькими.

Password Attacks – Means "password cracking" in English. This is the process of using software tools to determine an unknown or forgotten password to access a computer or network resource. Additionally, it can be used to help a threat actor gain unauthorized access to resources.

Malicious individuals can use information obtained through password cracking to carry out a range of criminal acts. These include stealing bank account or personal information, using the compromised device as a zombie for other malicious purposes, and fraud.

Password crackers use various methods to crack passwords. The process may involve comparing a list of letters to guess passwords or using an algorithm to repeatedly guess the password. A common type is the Brute Force program.

1. Brute Force - This attack is carried out by trying combinations of characters of a predetermined length until a match for the password is found.

2. Dictionary Search - Here, the password cracker searches for each word in a dictionary as the correct password. Password dictionaries exist for various topics and combinations of subjects, including politics, films, and music groups.

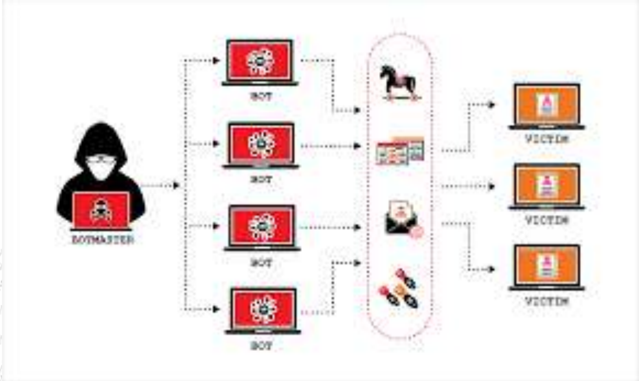
3. Phishing - These attacks are used to gain access to user passwords without using password cracking tools. Instead, the user is tricked into clicking on an email application. From there, the application may install malicious software or trick the user into using their email to log into a fake version of a website and reveal their password.

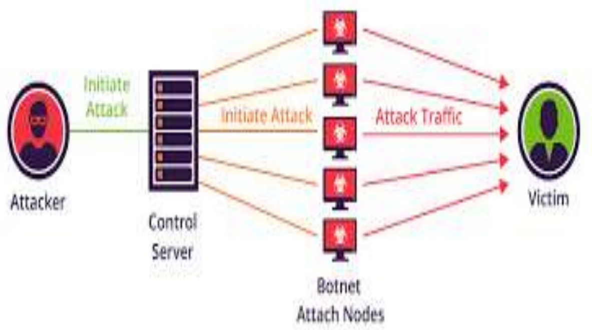
4. Malicious Software - Similar to phishing, using malware is another method of gaining unauthorized access to passwords without using password cracking tools. Instead, malicious software such as keyloggers that record keystrokes or screen scrapers that capture screen images are used.

5. Rainbow Table Attack - This approach involves using other words derived from the original password to generate other possible passwords. Malicious actors may maintain a list called a rainbow table. This list contains leaked and previously cracked passwords, making this common password cracking method even more efficient.

6. Guessing - A cracker may guess a password without using cracking tools. If the threat actor has enough information about the victim or if the victim uses a sufficiently common password, they may find the correct characters.

DDoS Attacks – A hacking attack to disable a computer system, i.e., sending harmful data to the system's users' computers, causing them to slow down or completely stop working, which aids in carrying out other cyberattacks. DoS (Denial of Service) is carried out via a single computer, while DDoS (Distributed Denial of Service), as the name implies, involves sending harmful data to the victim from two or more compromised computers, leading to slowed or frozen access to information resources (servers). For large companies and organizations, server downtime causes significant damage. But often this is a measure of economic pressure: loss of revenue-generating normal services, costs for settlements with the provider and attack mitigation measures significantly hit the target's pocket. Currently, DoS and DDoS attacks are among the most popular because they render victims inoperative and are used for data theft and disruption.

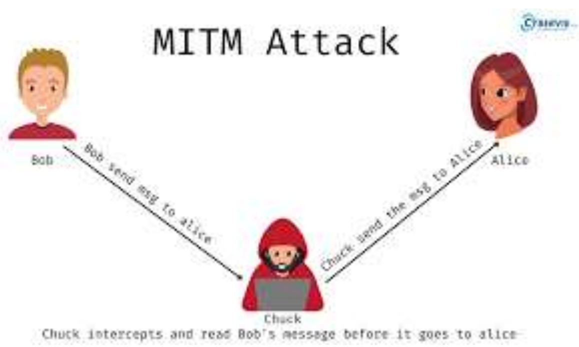


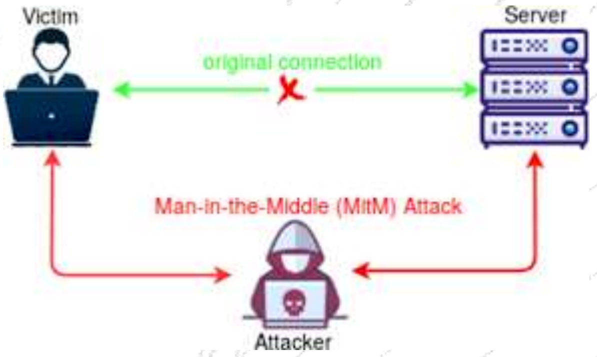


Man-in-the-Middle – (English “Man-in-the-Middle Attack”) is a cyberattack where an attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other, because the hacker inserts themselves between the two parties, controlling, receiving, altering, and downloading the data passing between them.

An active eavesdropping MITM attack involves the attacker establishing independent connections with the victims and relaying messages between them, making them believe they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker.

The attacker must be able to intercept all relevant messages passing between the two victims and have the capability to alter and download them. In many cases, an attacker within range of an unencrypted Wi-Fi access point can insert themselves as the man-in-the-middle.

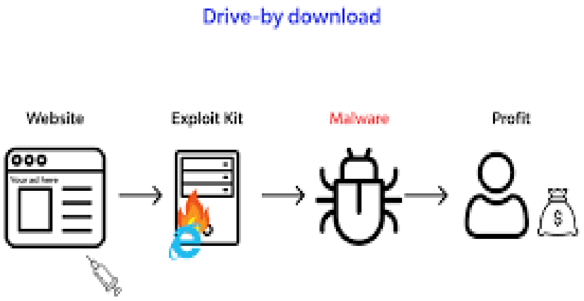

MITM Attack
Bob
Bob send msg to alice
Alice
Chuck send the msg to Alice
Chuck
Chuck intercepts and read Bob's message before it goes to alice

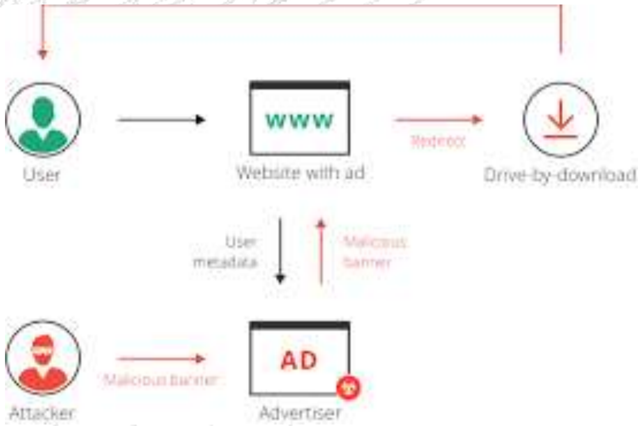


Drive-by Downloads – Downloads are of two types, both related to the unintended downloading of computer programs from the internet.

1. Authorized drive-by downloads – These are downloads that a person has authorized but does not understand the consequences of (e.g., downloads that install an unknown or fake executable program, an ActiveX component, or a Java application).

2. Unauthorized downloads – These are downloads that happen without the person's knowledge, often involving a computer virus, spyware, malicious software, or crimeware.





Malvertising (Malicious Advertising) – From the English "malware advertising," it means placing an interesting, attractive advertisement to lure victims. Upon clicking, without their knowledge, it places a virus inside, and over time, this computer or smartphone becomes a “**Zombie**,” allowing the hacker to use it at any desired time, extract information from it, or upload more malicious software.

Furthermore, in our country, we can observe several crimes such as Cyber Extortion, Cyber Fraud, Theft, and others, for example:

Cyber Extortion – Carried out by hackers by locking a phone or computer and threatening to make it disappear, or by accessing devices through other means, obtaining information, and using it as a weapon against the victim (e.g., personal information, compromising material, secrets) by demanding money.

Cyber Fraud Crime – Carried out by hackers through various programs and web pages by gaining the client's trust, then stealing their data, downloading programs, withdrawing money, and abusing their trust.

For example:

- Sending money to your plastic card, then asking you to send it back, in order to obtain your information, passwords, and withdraw money.
- Posing as a bank employee or government official, sending a request to obtain their information and passwords and withdraw money.
- Sending a link to direct them to a phishing site where they enter their information and plastic card codes, and that person becomes the victim.

Theft – This crime involves the perpetrator accessing the victim's computer or phone devices through illicit means, stealing information, secretly withdrawing money from the user's plastic card, and using it.

Email Phishing: Unlike general, mass-market phishing attacks, email phishing messages are sent to millions of potential victims in an attempt to deceive them and try to get them to log into fake versions of very popular websites.

Ironscales listed the most popular brands used by hackers in phishing attempts. Among over 50,000 fake login pages observed by the company] {.underline} these were the top brands exploited by attackers:

- PayPal: 22%
- Microsoft: 19%
- Facebook: 15%

References:

1. Anderson, R. (2022). Security Engineering: A Guide to Building Dependable Distributed Systems (3rd ed.). Wiley.
2. Schneier, B. (2015). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W. W. Norton & Company.
3. Furnell, S. (2021). Cybercrime: The Human Factor. CRC Press.
4. Holt, T. J., & Bossler, A. M. (2022). Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses. Routledge.
5. Yar, M., & Steinmetz, K. F. (2019). Cybercrime and Society (3rd ed.). SAGE Publications Ltd.
6. 1.6. Wall, D. S. (2015). Cybercrime: The Transformation of Crime in the Information Age. Polity Press.
7. Clough, J. (2015). Principles of Cybercrime (2nd ed.). Cambridge University Press.
8. Jaishankar, K. (Ed.). (2011). Cyber Criminology: Exploring Internet Crimes and Criminal Behavior. CRC Press.
9. Goodman, M. (2015). Future Crimes: Everything Is Connected, Everyone Is Vulnerable and What We Can Do About It. Doubleday.
10. Mitnick, K. D., & Simon, W. L. (2011). The Art of Deception: Controlling the Human Element of Security. Wiley.