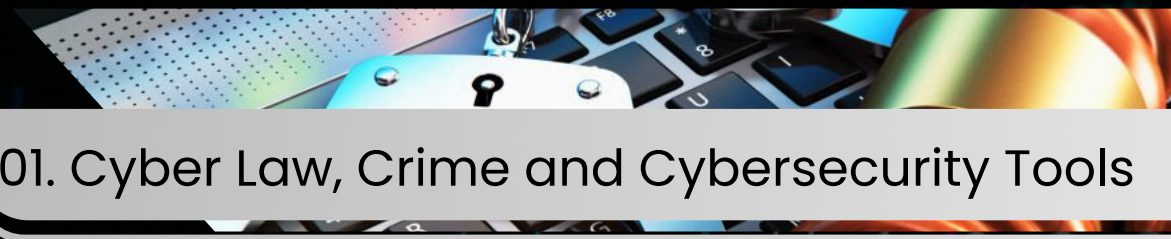
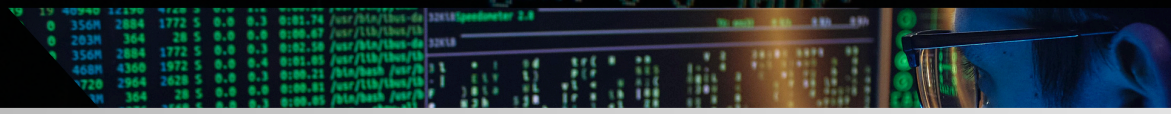
IN A DIGITAL WORLD WHERE EVERY ACTION LEAVES A TRACE AND DATA DEFINES WORTH, CYBERSECURITY STANDS AS THE CORE OF TRUST, STABILITY, AND ONLINE FREEDOM.

TECH FORTRESS 5.0

Published By
Community of Cybersecurity in Horizon

CONTENTS





CYBER LAW AND CYBER CRIME & TOP CYBERSECURITY TOOLS

By 2025, the use of AI was at an all-time high, and along with it, the use of security measures was widespread. Experts have said that about $10.5 trillion was spent on cybercrime last year due to the lack of proper security measures.

This article discusses some of the important cybercrime laws and high-end security tools in 2025.

Cyber Laws and Cyber Crime

There have been many major attacks in 2025. For example, a group called Medusa recently stole patient records from a medical company and demanded $1 million. Governments are creating new laws to combat these.

In Europe,

- NIS2: The second Network and Information Security Directive is an EU-wide legislative framework designed to strengthen cybersecurity requirements
- DORA: This law was created for banks and finance companies. They must test security and manage risks from other companies they work with.

In USA,

- CIRCIA: The Cyber Incident Reporting for Critical Infrastructure Act of 2022 is a U.S. federal law that requires timely reporting of significant cyber incidents, including ransomware attacks and ransom payments.

These laws mandate data protection, early notification of problems, and accountability. Companies that do not follow these laws face hefty fines.

These laws also make it easier to catch criminals. Police across the country are working together to stop hacker groups.

TOP 10 CYBERSECURITY TOOLS IN 2025

- **Wireshark**: This is a free tool that analyses network traffic in real-time for Windows, MacOS, Unix, and Linux systems.
- **Nmap**: This is an open source tool used by cybersecurity professionals to discover hosts, map networks, and identify potential security vulnerabilities.
- **Metasploit**: This tool is a widely used penetration testing framework that enables security teams to identify and exploit vulnerabilities in networks, systems, and applications.
- **Burp Suite**: This tool is a proprietary software tool for security assessment and penetration testing of web applications.
- **Kali Linux**: This is a Linux distribution designed for digital forensics and penetration testing.
- **Nessus**: This is a proprietary vulnerability scanner developed by Tenable, Inc for improving the integrity of a network.
- **Splunk**: This tool is used for monitoring network security , data analysis and incident response.
- **Snort**: This is an open source tool used to scan networks and prevent any unauthorized activity in the network.
- **KisMAC**: This is a wireless network discovery and security assessment tool designed for monitoring and analysing Wi-Fi networks on macOS systems.
- **Forcepoint**: This is a security tool, primarily meant for cloud users.

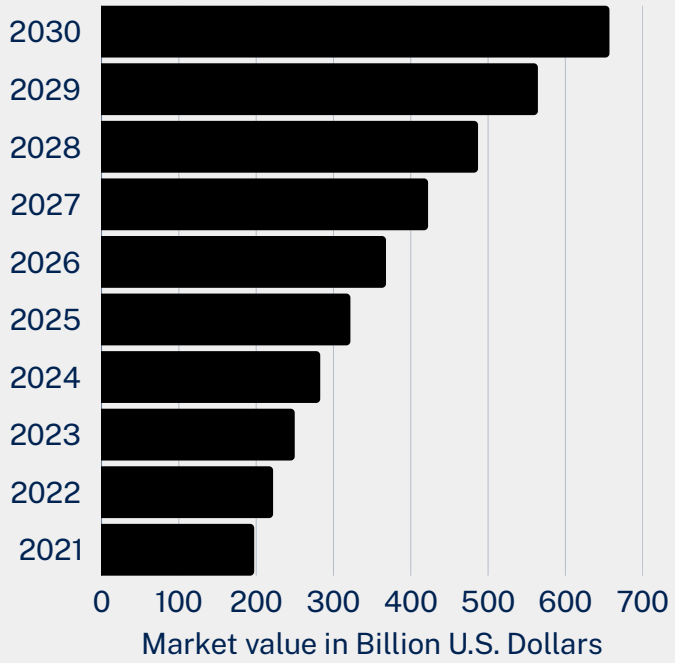
Using these tools, you can perform vulnerability scanning, penetration testing, incident response, and real-time monitoring, which are very important for operational security in a complex digital environment. Therefore, you should invest in new security tools and understand the digital rules.

THE FUTURE OF CYBERSECURITY JOB

A Booming Frontier

In a world where digital connectivity underpins business, government, and personal life, cybersecurity has risen from a specialized technical field to a core necessity. As cyberattacks become more frequent, sophisticated, and costly, the demand for a workforce capable of securing digital infrastructure continues to grow stronger each day.

Predicted Size of Cybersecurity Market Worldwide from 2021 to 2030



A Growing Global Demand

Cybersecurity positions are expanding rapidly worldwide. According to various industry predictions, it was predicted that by 2025 there would still be millions of unfilled cybersecurity roles globally, driven by the growing need to secure everything from personal data to critical infrastructure. As a result, cybersecurity job openings are expected to grow at a strong pace, with some areas projected to see growth of more than 30% over the next decade—significantly higher than the average across most industries.

WHAT ROLES ARE DEFINING THE FUTURE?

The cybersecurity network is a system of various players which keeps changing with time. Some of the most interesting roles that are getting more and more important include:

Cybersecurity Analyst
A cyber security analyst keeps an eye on networks, looks into incidents and threats and generally tries to mitigate the effects of the attacks. They are usually the first line of the network which is protective against assaults.

Ethical Hackers / Penetration Testers
Normally, these experts try to think from the perspective of the attackers so that they can find the loop holes and fix them before any ill-intentioned hackers take advantage of them.

Cloud Security Engineers
It is very important to secure cloud environments as more companies are switching to cloud platforms.

AI Security Specialists
The rise of artificial intelligence as a tool and a threat calls for the experts that can ensure the security of AI systems. Such specialists are the most valuable.

Incident Responders & Threat Hunters
These professionals identify the parts of the system that were compromised and stop the spread of the breach. They also look for the source of the attack, the most sophisticated threat.
Apart from these, positions that concentrate on privacy compliance, security automation, and cyber policy are also coming up as the professionals of the future.

Artificial Intelligence's Role

In cybersecurity, artificial intelligence presents both advantages and challenges. On one hand, defenders use AI technologies to automate repetitive tasks and detect threats more quickly. On the other hand, attackers are leveraging AI to create increasingly sophisticated threats. As a result, cybersecurity professionals must continually adapt and acquire new skills to stay ahead.

Challenges Ahead

Although there are many potentials, there are also difficulties in the cybersecurity field

Skills Gap
Many businesses are under staffed, especially in specialized areas, due to a continuous lack of competent workers

Stress & Burn out
Some teams may experience stress and turn over as a result of the strain of defending against persistent threats. (Industry reports indicate that the career is very stressful)

Changing Threat Landscape
As 5G networks, AI, and IoT (Internet of Things) expand, so do the opportunities for cyberattacks, necessitating on going skill development on the part of defenders.

Competitive Salaries

In general, cybersecurity positions promise a good income that will increase swiftly with one's experience and further specialization. Although exact figures differ from one country and role to another, forecasts indicate considerable increases in remuneration over the next ten years.

Meanwhile, entry-level wages remain attractive in regions with developing economies, and senior leadership roles such as Chief Information Security Officer (CISO) are expected to be highly compensated as organizations increasingly recognize cybersecurity as a critical strategic priority.

The Bottom Line

Jobs in cybersecurity are expected to grow and evolve significantly in the coming years. This creates strong demand for skilled professionals, with competitive global wage rates for both experienced workers and students entering the field.

Cybersecurity is a dynamic and ever-evolving field that offers a wide range of roles and significant opportunities to specialize in areas such as threat intelligence, cloud computing, and artificial intelligence. As digital risks continue to evolve and the global cyber-threat landscape becomes increasingly complex, cybersecurity is positioned to be one of the most fascinating and resilient career paths over the next decade.

THE PSYCHOLOGY OF HACKING

What is the Psychology of Hackers?

Although many people think hacking is technical, it's both technical and psychological. The intent behind every cyber-attack comes from the human mind, which is influenced by creativity, feelings toward others, and a desire for something more than they currently have. It's important to know about the psychology of hacking to find out not only how hackers operate but also why they hack do so.

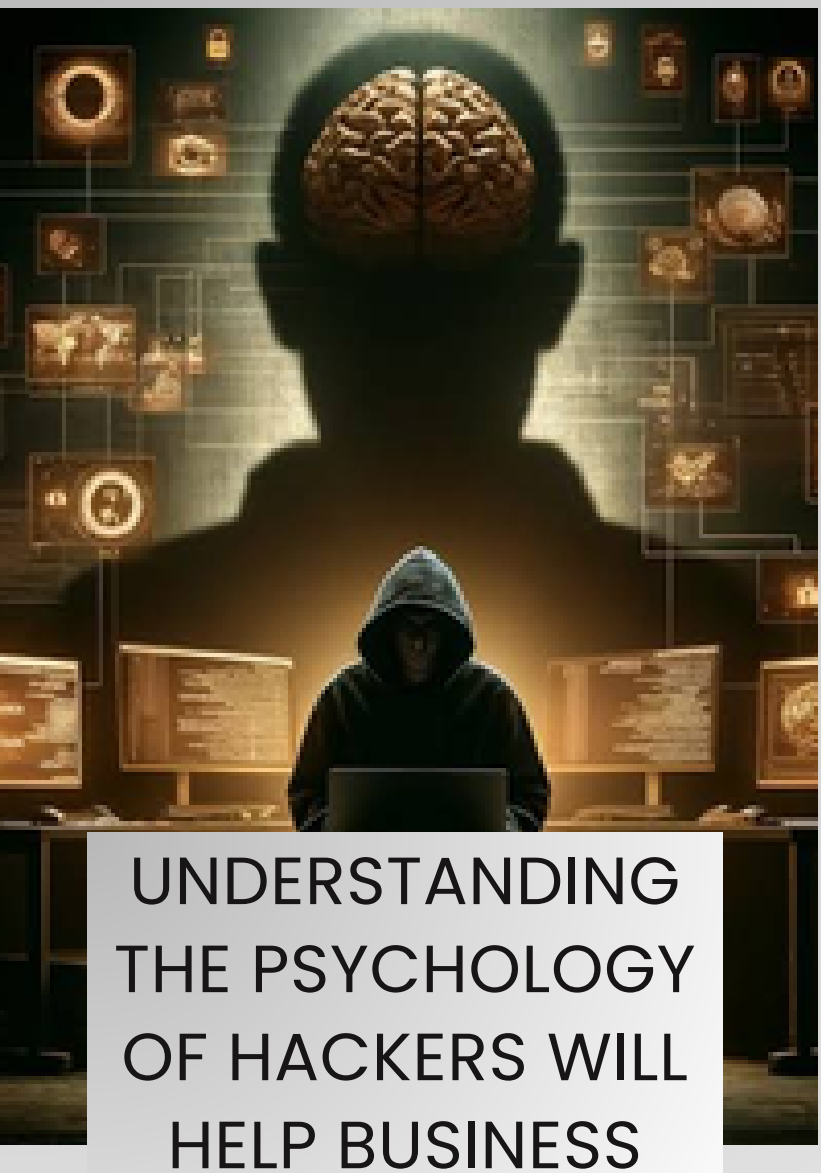
Mindset of Hackers

A hacker's way of thinking includes curiosity, a sense of creativity, and a need to go beyond established limits. In this chapter, we look at the psychological characteristics that make up this mindset and how they affect hacking actions.

"Ransomware is more about manipulating vulnerabilities in human psychology than the adversary's technological sophistication."

James Scott

TYPES OF HACKERS	DRIVING PSYCHOLOGICAL FORCES
White Hat	Duty, Ethics, and the desire to Keep Learning
Black Hat	Greed, Revenge, Thrill-seeking
Grey Hat	Curiosity and risk-taking
Script Kiddie	Thrill, Peer Approval



UNDERSTANDING THE PSYCHOLOGY OF HACKERS WILL HELP BUSINESS OWNERS

- **Build more effective Cybersecurity Awareness Programs**
- **Increase the effectiveness of Ethical Hacking Education**
- **Anticipate and counteract Cyber Threats before they occur**
- **Diminish insider & social engineering attacks**

The combination of technology and human factors in cybersecurity will enhance the effectiveness of cybersecurity programs.

THE PSYCHOLOGICAL IMPACT OF HACKING

The psychological impact of hacking includes positive, negative, and chaotic associations for hackers as they execute their attacks. Hackers often feel excitement, satisfaction, or adrenaline rush from performing successful hacks. This creates patterns of behavior that continue as hackers grow accustomed to engaging in these attacks, and this experience may eventually lead to the decreased ability to justify their unethical behavior. For victims of hacking, there are many implications on their mental health, including stress levels, fear, financial loss, and diminished trust in digital technologies.

CRYPTO WALLET SECURITY

What is crypto wallet?

A crypto wallet is an application that functions as storage for your cryptocurrency. And also we can describe that like, a crypto wallet because it is a tool that allows you to store, manage, and interact with digital currencies like Bitcoin and Ethereum. It is called a wallet because it is used similarly to the traditional wallet you use to organize cash and cards. Instead of holding these physical items, it stores the passkeys you use to sign for your cryptocurrency transactions and provides the interface that lets you access your crypto. Instead of holding the actual coins, a wallet stores your cryptographic keys, which give you access to the cryptocurrency recorded on a blockchain. Modern crypto wallets make the blockchain accessible to everyone.

How does that work?

Cryptocurrency wallets are software applications on computers or mobile devices. They use an internet connection to access the blockchain network for the cryptocurrency you're using.

Cryptocurrencies are not "stored" anywhere, they are bits of data in a database, scattered all over it. The wallet finds all of the bits associated with your public address and sums up the amount for you in the app's interface.

Sending and receiving cryptocurrency is very easy using these applications. You can send or receive cryptocurrency from your wallet using various methods.
Receiving is even easier; the sender enters your address and goes through the same routine.

TYPES OF CRYPTO WALLETS

Two types of crypto wallets are available

Custodial wallets: The custodial wallet is managed by a third-party entity, like a bitcoin exchange. In this arrangement, the supplier holds and protects the private keys on your behalf.

Non-custodial wallets: In a non-custodial wallet, your private keys are entirely under your control and you are the sole owner of your cryptocurrency. A third party cannot access, manage, or freeze your funds.

Additionally, wallets for cryptocurrencies come in two varieties

Hot wallets: Software-based wallets that are accessible online. They offer instant, real-time access to your cryptocurrencies and are perfect for regular users.

Cold wallets: Long-term storage and the highest level of protection are the goals of these offline wallets.

Finally, there are three other subcategories of cryptocurrency wallets

Software wallets: These are desktop or mobile applications. They strike a balance between practicality and usability.

Paper wallets: Your public and private keys are printed out on paper, sometimes as QR codes.

Hardware wallets: Hardware wallets are actual gadgets that save your private keys separate from your computer or phone in a safe chip. Ledger Nano S/X and Trezor Model T are two well-known models.

Basic Items of Crypto Security

The following are the essential items needed to secure cryptocurrencies:

•Private Keys and Public Keys - A private key is a unique code used to spend your cryptocurrency, whereas a public key is an address that can be accessed by anyone and can be used as a destination for sending and receiving cryptocurrency.

•The difference between Cold and Hot Wallets - Cold wallets provide a way to store your crypto assets offline, while hot wallets are designed for online access, but are subject to hacking threats and your assets could potentially be lost permanently.

•Regular updates - Software updates for crypto wallets should be done on a regular basis to address potential vulnerabilities and prevent security breaches.

Why are cryptocurrency wallets important?

Cryptocurrency wallets are important because they provide you with a foundation for participating in the digital asset economy.

- **Security-** It protects your private keys, so only you have the authority to sign for transactions. Wallets protect your funds through the use of encryption, PINs, and biometric login.

- **Ownership-** A non-custodial wallet allows you to truly be financially independent.

- **Transaction control-** You are able to send and receive crypto at any time without having to ask a bank or other intermediary for permission.

- **Functionality/ Access-** The wallet is not just the key to the Web3 ecosystem. It also serves as the gateway to NFTs and participation in DeFi.

Each cryptocurrency is supported by the technology behind cryptocurrency security, which provides a means for recording and verifying each cryptocurrency's transactions and verifying the ownership to be recorded in a secure, decentralized manner on behalf of all members of the crypto community.

HOW TO KEEP YOUR CRYPTOCURRENCY WALLET SECURE?

Security is essential when managing your own crypto. Here are key steps to keep your wallet safe:

Use strong unique passwords and store them in a secure password manager

Protect your private key and recovery phrase, never store them in plain text or online

Stay alert for phishing emails, fake apps, and malicious links impersonating wallet services.

WHAT ARE THE CRYPTO WALLET THREATS?

Cryptocurrency has revolutionized the financial world. Around the world, 562M people use online finances because they prefer to decentralized and secure transactions. Unfortunately, with great innovation comes significant risks. Now let's see what are these,

Phishing Attacks

Most successful data breaches start with a phishing attack. This threat is extremely common and effective. Cybercriminals use deceptive emails, messages, or websites that mimic legitimate entities to trick users.

Malware and Ransomware

Including keyloggers and clipboard hijackers, can capture your login credentials or alter wallet addresses during transactions. Ransomware steals and encrypts your data so that only those with the right decryption key can access it.

SIM Swapping

SIM swapping involves attackers taking control of your phone number by tricking or bribing telecom employees. Once they have control, they can bypass SMS-based MFA and access your cryptocurrency accounts.