Cyber Security

2024

The Bad Guys You must Defend Against

Vathna.lay@cadt.edu.kh

Beyond Basic Attacks: Advanced Threats

- **Rootkits**: Hidden tools that give attackers deep control of your computer, often undetectable by regular security.
- **Brute-force attacks:** Trying every possible combination until they crack your password.
- **Injection attacks:** Sneaking malicious code into a system's input.
- **Cross-site scripting (XSS):** Planting harmful code on a website you trust, so it infects your device when you visit.

Beyond Basic Attacks: Advanced Threats

- **SQL Injection:** Sneaking code into database queries to steal or manipulate information.
- **Session Hijacking:** Taking over your online session with a website.
- **Malformed URLs:** Tricky web links that look harmless, but actually lead to malicious sites or trigger system errors.
- **Buffer Overflow Attacks:** Overloading a program's memory with data, causing it to crash or execute hidden commands.

Scenario 1: The Hidden Admin

A tech-savvy employee notices their computer is running unusually slowly. Task Manager shows unknown processes consuming resources, and some files are inexplicably disappearing. Antivirus scans turn up nothing.

Question: What kind of attack could be causing this?

Rootkit

Scenario 2: Login Mania

A website administrator notices a sudden surge in failed login attempts from different IP addresses. They realize these attempts are trying every combination of letters and numbers.

Question: What kind of attack could be causing this?

Brute Force

Scenario 3: The Unexpected Comment

A popular online forum suddenly starts displaying strange pop-ups and redirects to malicious sites whenever users click on certain comments.

Question: What kind of attack could be responsible for this?

Scenario 4: The Website Meltdown

A company website crashes unexpectedly after a user submits a long, complex form with strange characters in several fields.

Question: What type of attack could have caused the crash?

SQL INJ

Scenario 5: The Bank Transfer Mystery

A user tries to transfer funds from their bank account online. They type in the correct website address, but end up on a page that looks slightly different. The page asks for their login credentials, which they enter. Later, they discover unauthorized transactions have taken place.

Question: What kind of attack might have happened?

Malformed URL

Scenario 6: The Vanishing Shopping Cart

A user is browsing an online store, adding items to their shopping cart. Suddenly, they are logged out and their cart is empty. When they try to log back in, their password doesn't work.

Question: What could explain this sudden loss of access?

Scenario 7: The Strange Twitter Link

A user receives a direct message on Twitter from a friend, containing a link to a news article.

The link looks odd, with lots of special characters. When they click it, their browser crashes.

Question: What type of attack might this be?

Buffer overflow

Scenario 8: The Unexpected Shutdown

A company server suddenly crashes. Upon investigation, the IT team finds that the server's memory was overloaded with unexpected data, causing critical processes to fail.

Question: What kind of attack could have caused this overload?

Buffer Overflow

Good Guys vs. Bad Guys in Cyberspace

- **Online morality is relative**
  - What you consider a cyberattack, others might see as heroism.
  - Cultural and ideological differences lead to varying views on what constitutes good and bad online behavior
  - Even within a single culture, there can be deep divides over what is acceptable.
- **Who are the Good Guys and Bad Guys?**
  - For the purpose of self-defense in cyberspace, anyone seeking to harm your interests is considered bad.
  - This definition is subjective and focused on protecting your digital assets and privacy

Types of Attackers

- **Script Kiddies**: Inexperienced hackers using readily available tools.
- **Kids who are not Kiddies**: Young, tech-savvy individuals with malicious intent.
- **Nations and States**: Government-backed hackers pursuing political or economic agendas.
- **Corporate Spies**: Seeking to steal trade secrets or gain competitive advantage.
- **Criminals**: Motivated by financial gain through fraud, extortion, or theft.
- **Hacktivists**: Driven by ideological or political causes, often using cyberattacks to disrupt or expose.

Cyberattackers & Their Colored Hats

Malicious intent. Hack to steal, manipulate, or destroy.

Ethical hackers. Hack to test and improve security with permission.

No malicious intent, but may act unethically or illegally.

Novices seeking to become experts.

Paid to test software for bugs before release.

Which color?

A hacker discovers a security flaw in a social media platform and publicly discloses it, putting pressure on the company to fix the issue quickly.

Which color?

A hacker breaches a company's database to steal customer credit card information, then sells it on the dark web for profit.

Which color?

A hacker participates in online hacking challenges and forums to learn new techniques and improve their skills.

Which color?

A government agency employs hackers to find vulnerabilities in critical infrastructure systems and ensure their resilience against cyberattacks.

White

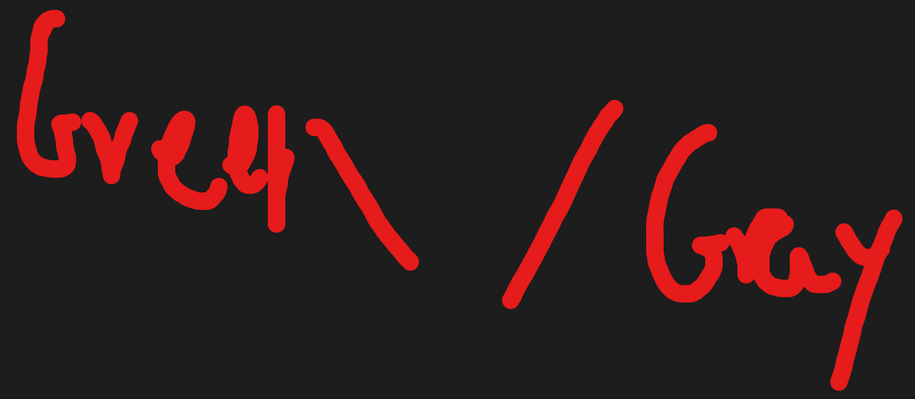
Which color?

A software company hires a hacker to test a new product for security flaws before its official release.

Blue

Which color?

A hacker experiments with building basic hacking tools and scripts to understand how vulnerabilities are exploited



Which color?

A hacker accesses a company's systems without authorization, but instead of causing harm, they notify the company of the vulnerability and offer to fix it for a fee

White

Which color?

A hacker deploys ransomware on a hospital's network, encrypting crucial patient data and demanding a ransom for its release

Which color?

A cybersecurity firm hires a hacker to conduct a penetration test on their client's network to identify vulnerabilities before attackers can exploit them.

Which color?

A hacker discovers a critical vulnerability in a popular software program and responsibly discloses it to the vendor, allowing them to patch the issue before it's exploited.

White

How Cybercriminals Monetize Their Actions

Direct Financial Fraud: How Hackers Steal Your Money

- Traditional Method
  - Malware captures online banking sessions.
  - Hackers redirect funds to their accounts.
- Shifting Targets
  - Criminals target less secure systems (coffee shop apps, reward programs).
  - Steal stored value or credits for goods/services.
  - Stolen credit card numbers used or sold for fraudulent purchases.

How Cybercriminals Monetize Their Actions

Beyond Direct Theft: Cybercriminals' Strategies for Indirect Financial Fraud

- Direct fraud yields smaller payouts.
- Victims can often reverse transactions or invalidate fraudulent orders.
- Higher risk of getting caught.

Indirect financial fraud

Profiting off illegal trading of securities

- **Pump and Dump**
  - Hack companies, steal data, short-sell stock, leak stolen data to crash stock price, or buy back stock at lower price for profit.
- **Bogus Press Releases & Social Media Posts**
  - Manipulate stock prices by releasing false news through hacked channels
- **Insider Information**
  - Steal unreleased financial information or press releases, then trade securities based on insider knowledge for unfair advantage.

Indirect financial fraud

Stealing Payment Information: Cybercriminals' Lucrative Business

- **Target: Credit/debit card numbers, other payment details**
- **Methods:**
  - Malware, phishing scams, data breaches, skimming devices
- **Usage:**
  - **Direct Purchases:** Goods, services, gift cards, software
  - **Reselling Stolen Data:** Dark web marketplaces for quick profit before detection
  - **Exploitation by Others:** Criminals with infrastructure for maximizing fraud before cards are blocked

Indirect financial fraud

Theft Beyond Money: Cybercriminals Targeting Goods & Data

- **Targeting High-Value Goods:**
  - Criminals track orders of jewelry and other small, valuable items.
  - Intercept deliveries or steal from recipients directly.
- **Data as a Commodity:**
  - **Financial Crimes**: Stolen data used for identity theft, fraud, or extortion.
  - **Dark Web Sales:** Personal information, financial details sold for profit.
  - **Corporate Espionage:** Stolen data valuable to competitors, causing financial harm.
  - **Public Leaks:** Damage reputation, disrupt operations, or expose secrets.

Not All Dangers Come From Attackers

The weakest link:

- Human error is a major contributing factor in almost all major cyber breaches.
- It's often the crucial element that enables hostile actors to succeed.

What are the Forms of Human Error?

Humans: The Achilles' Heel of Cybersecurity

- **Why are humans the weakest link?**
- **Consequences:**
  - Human error leads to major security breaches.
  - Hackers exploit human weaknesses through social engineering.
  - Mistakes like weak passwords, phishing scams, and misconfigurations compromise security.

Question

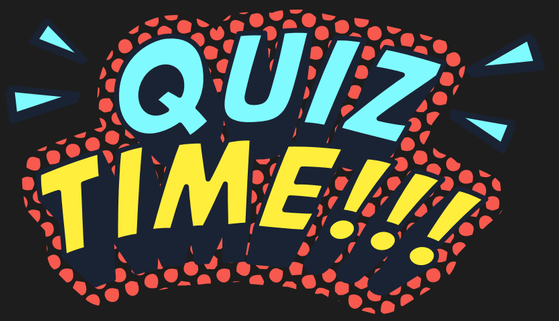
Which type of hacker is motivated by financial gain and often engages in direct financial fraud?

A. White hat hacker

B. Gray hat hacker

C. Black hat hacker

D. Green hat hacker



Question

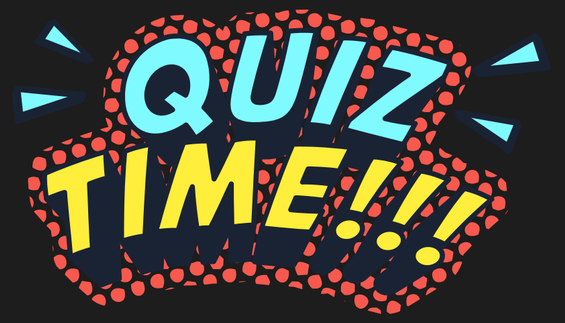
Which of the following is an example of indirect financial fraud?

A. Stealing credit card information and using it to make purchases.

B. Hacking into a company's bank account and transferring funds.

C. Selling stolen personal information on the dark web.

D. Installing malware on a victim's computer to capture banking credentials.



Question

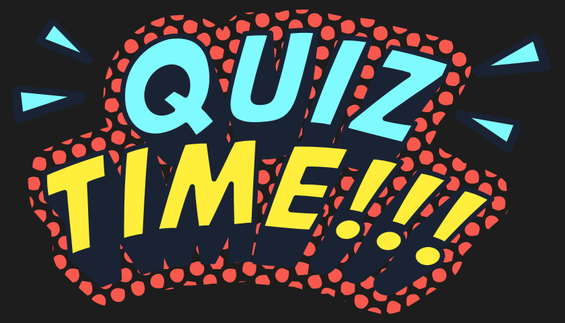
What is the primary weakness exploited by cybercriminals in most major breaches?

A. Outdated software

B. Weak passwords

C. Human error

D. Unpatched vulnerabilities



Question

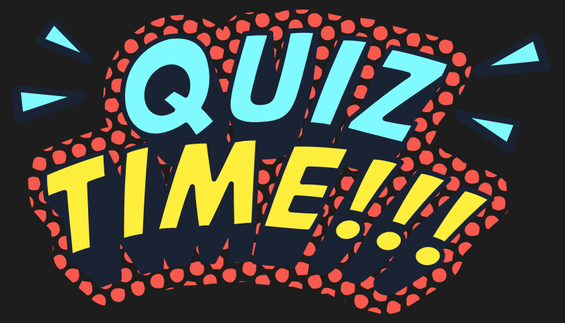
Which type of cybercriminal is most likely to engage in pump-and-dump schemes involving securities?

A. Corporate spies

B. Hacktivists

C. Script kiddies

D. Nation-state actors



Question

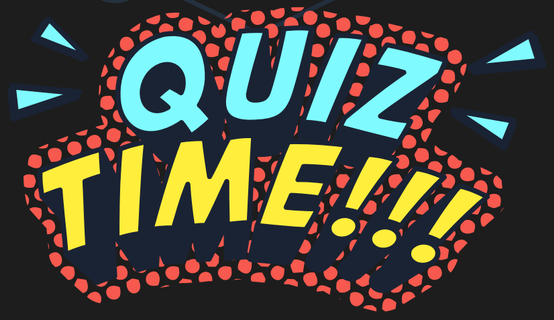
What is the main reason sophisticated cybercriminals prefer indirect financial fraud over direct fraud?

A. It's easier to execute.

B. It's less risky and harder to trace.

C. It yields higher immediate payouts.

D. It requires less technical skill.



Question

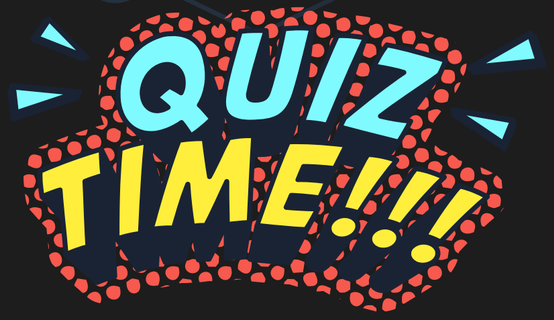
Which type of hacker is often hired by companies to test their security systems?

A. Black hat hacker

B. Gray hat hacker

C. White hat hacker

D. Blue hat hacker



Question

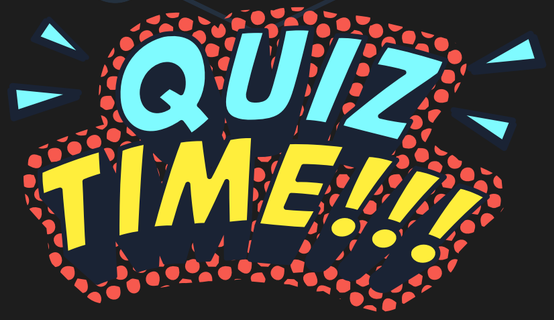
Which of the following is NOT a reason why humans are the weakest link in cybersecurity?

A. The rapid pace of technological advancement.

B. The increasing complexity of devices and systems.

C. The growing number of passwords and logins to manage.

D. The inherent strength of the human brain compared to technology.



Question

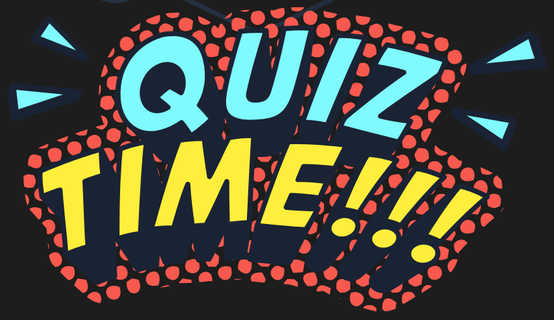
Which type of cybercriminal is typically a novice seeking to learn and improve their skills?

A. Black hat hacker.

B. Gray hat hacker.

C. Green hat hacker.

D. Blue hat hacker



Question

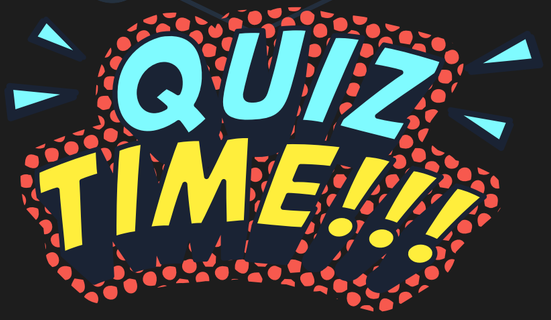
What is the main benefit for attackers when using malvertising?

A. They can directly steal money from user accounts.

B. It allows them to bypass a user's security software.

C. They can infect a large audience through trusted websites.

D. Malvertising is a cheap and easy way to launch cyberattacks.



Question

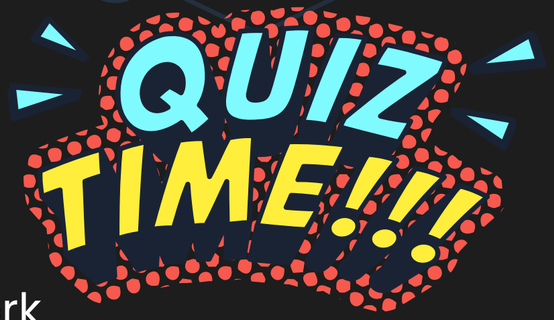
What is the main difference between a blue hat hacker and a white hat hacker?

A. Blue hat hackers are paid to test software before release, while white hat hackers test systems already in use.

B. Blue hat hackers are malicious, while white hat hackers are ethical.

C. Blue hat hackers work for government agencies, while white hat hackers work for private companies.

D. Blue hat hackers use only manual testing methods, while white hat hackers rely on automated tools.




?
Q&A