INSIDE THE HACKER'S MIND

Zain Javed, Chief Technology Officer at Citation Cyber, considers the psychology of cyber attacks and how to outsmart the hackers

Can you really protect yourself from hackers without first understanding them? That means more than knowing what malware looks like or spotting suspicious emails. It means stepping into the mindset of someone whose day revolves around finding weaknesses, exploiting them and turning them into opportunity.

Cyber attacks are rarely random bursts of malicious code. They are deliberate, calculated and often deeply personal. Every attack has a human behind it – patient, persistent and prepared to exploit your technology and your people.

If you want to stay safe now, and in the future, you have to think like the person searching for a way in.

The word hacker often conjures images of shadowy figures in hoodies hunched over glowing screens. The reality is far more complex.

There is a wide spectrum of different types:

- **Black hat hackers:** These are the cybercriminals you read about in the headlines. They break into systems for profit, political gain or personal vendettas.
- **Grey hat hackers:** Skilled individuals who might break the law but often claim to do so for the greater good – exposing vulnerabilities to push organisations into fixing them.

Continued overleaf >>

SHARE WITH YOUR NETWORK

>> From previous page

- **White hat hackers:** The ethical professionals who use their skills to strengthen security, often working as penetration testers or researchers.

Their motives vary:

- Some hack for **money**, launching ransomware attacks or stealing personal data to sell.
- Others are driven by **ideology** or activism, seeking to disrupt organisations they oppose.
- A few hack for the **thrill** of it – the intellectual challenge of bypassing defences.

And now, there's a new driver in the mix: access to powerful artificial intelligence (AI) tools that allow even unskilled attackers to generate convincing phishing emails, deepfake voices or malicious code in seconds and lowering the barrier to entry for cybercrime.

To beat a hacker, you must recognise the traits that make them so effective. These are:

1. Patience and persistence

Many cybercriminals will spend weeks – even months – studying a target before making a move. They'll research your employees on LinkedIn, follow your company on social media and quietly probe your systems for weaknesses. They play the long game because one well-timed, well-crafted attack is worth far more than dozens of rushed attempts.

2. Creative problem-solving

Hackers are natural puzzle-solvers. If they encounter a blocked path, they look for another route – maybe a forgotten test server or a supplier's less secure network. They think sideways, not just straight ahead.

3. Empathy inversion

Hackers often put themselves in someone else's shoes, not to help them, but to manipulate them. They understand what will scare, flatter or pressure you into clicking that link or sharing that password.

4. Risk versus reward calculation

Just like any business, attackers weigh their options. Which target offers the biggest payoff for the least risk? If your cyber defences are minimal, you may find yourself at the top of their list.

5. Testing boundaries

For some, the thrill lies in seeing what's possible. They push against rules, limits and safeguards – working not just for profit, but for the rush of beating the system.

HACKING PEOPLE, NOT MACHINES

When we picture hacking, we imagine lines of code flashing on a screen. But many attacks begin not with a technical exploit, but with a simple conversation, email or phone call.

This is social engineering – the art of manipulating people into giving up information or access. Why bother breaking through a secure firewall when you can convince an employee to open the door for you?

Common tactics include:

- **Phishing:** Emails or messages designed to look legitimate, tricking you into clicking malicious links.
- **Spear phishing:** Targeted attacks aimed at specific individuals, using personal details to build trust.
- **Pretexting:** Inventing a scenario – for example, posing as IT support – to obtain sensitive data.
- **Baiting:** Offering something enticing (like a free download) that hides malicious software.
- **Tailgating:** Physically following someone into a secure building.

The psychology is simple yet powerful. Attackers play on fear ('Your account will be closed!'), urgency ('You must act now!'), trust ('This is your boss'), and curiosity ('Click here to see the report').

A STEP-BY-STEP ATTACK

Every hack will follow the same steps. Let's break down an example.

Stage 1 – Reconnaissance:

A hacker chooses a small marketing firm that works with several large retail clients. They

66%

of security leaders say AI-driven attacks are their fastest-growing concern

(Source: Forrester, 2024)

DEEPFAKE-ENABLED FRAUD ATTEMPTS ROSE BY 3,000% BETWEEN 2022 AND 2024.

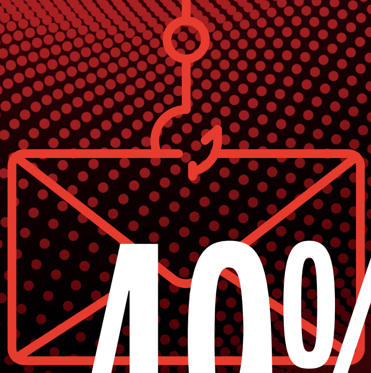
(Source: Sumsub, 2024)

95%

of cyber security breaches involve human error

(Source: IBM Cyber Security Intelligence Index)

83



49%

of phishing emails are now AI-generated, making them harder to detect

(Source: Darktrace, 2024)

AI-ASSISTED MALWARE DEVELOPMENT IS **GROWING AT 135% YEAR-ON-YEAR**

(Source: NCC Group, 2024)

1 in 4

companies have already faced an attack involving AI-generated social engineering

(Source: Proofpoint, 2024)

PHISHING IS THE **#1 CAUSE OF REPORTED SECURITY INCIDENTS** GLOBALLY

(Source: Verizon 2024 Data Breach Investigations Report)

%

OF ORGANISATIONS EXPERIENCED A PHISHING ATTACK IN THE LAST 12 MONTHS

(Source: Proofpoint 2024 State of the Phish)

follow employees on LinkedIn and discover that Sarah posts regularly about her projects.

Stage 2 – Crafting the approach:
Using details from her posts – and with help from an AI writing tool to mimic corporate tone – the attacker sends Sarah a personalised email that appears to be from a retail client's marketing director. It contains a draft campaign brief in PDF form.

Stage 3 – The hook:
Sarah opens the file. It contains a malicious macro (virus) that installs a remote access tool on her computer.

Stage 4 – The breach:
The attacker uses this access to explore the firm's systems, eventually stealing credentials for a client's e-commerce platform.

Stage 5 – The payoff:
The hacker uses the stolen access to skim payment details from hundreds of customers before being detected.

At every stage, AI enhanced the realism, speed and scale of the attack. Fighting cybercrime now means preparing for the human element and the machine element. So how can you prevent cyber attacks?

1. Train like you mean it

Generic tick-box cyber training doesn't work. Employees need engaging, scenario-based sessions that replicate real-life – and AI-enhanced – attacks, including deepfake voice calls and AI-generated phishing.

2. Test your defences

Regular penetration testing reveals weaknesses before criminals find them. Ask testers to include AI-assisted attack simulations in their scope.

3. Build layered security

Combine technical safeguards (multi-factor authentication, intrusion detection) with process controls (strict onboarding/offboarding, supplier vetting). AI can be your ally too – in the form of behaviour analytics and anomaly detection.

4. Create a culture of questioning

Employees should feel confident challenging unusual requests, even from senior leaders – especially if the 'leader' is on video or audio.

5. Stay ahead of the curve

Monitor cybercrime trends and AI developments. What worked before may be obsolete today.

THE ROAD AHEAD

The cyber security landscape has always been in motion, but AI is accelerating that change. In the coming years, expect:

Hyper-targeted attacks

AI can analyse vast amounts of public data to craft personalised attacks at scale. Imagine phishing emails tailored not just to your name, but to your job role, recent projects and even writing style.

Voice and video impersonation at scale

Deepfake technology will make CEO fraud harder to spot. Soon, it will not just be senior leaders – AI could convincingly imitate colleagues, clients or even family members.

Automated vulnerability discovery

Attackers will use AI to continuously scan for and exploit weaknesses the moment they appear – dramatically shrinking the window organisations have to patch systems.

AI-on-AI combat

Just as attackers deploy AI offensively, defenders will rely on AI-driven monitoring, threat hunting and automated response. The future of cyber security will be as much machine vs machine as human vs human.

Regulation and ethical challenges

Governments will struggle to keep pace. Expect debates over banning certain AI capabilities, as well as the ethics of using offensive AI tools for defensive research.

The psychology of the hacker is evolving. Where once they relied solely on patience, creativity and manipulation, they now have an intelligent partner that never sleeps, learns fast and can operate at a scale no human can match. Understanding this combined human–AI mindset will be the defining security challenge of the next decade.

You don't need to become a hacker to beat one, but you do need to learn how they think.

Citation Cyber is a dedicated cyber security partner for UK organisations, offering tailored support to strengthen digital resilience and reduce cyber risk. Combining human expertise with smart technology, Citation Cyber delivers services including Cyber Essentials certification, vulnerability scanning, phishing simulations, penetration testing and employee awareness training. Citation Cyber is part of the Citation Group, a leading provider of health and safety and HR and employment law services across the UK. **www.citationcyber.com**