Phriendly Phishing

PODCASTS

BYTES

WITH BEC & BENJI

Cyber Attacks and Digital Forensics Incident Response (DFIR)

How do you investigate a cyber crime?

Our guest...

Nick Klein

Executive Director
Cyber Resilience
CyberCX

Phriendly Phishing

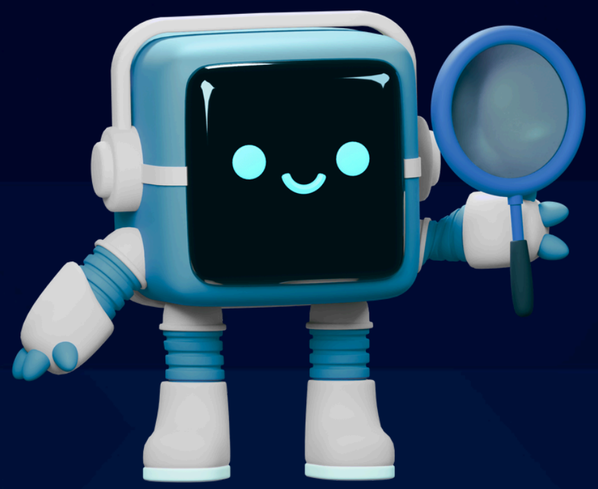
PODCASTS

THE BYTES

- **What is Digital Forensics and why's it important?**
  - Digital forensics is crucial for investigating cybercrime, data breaches, and security incidents by identifying, preserving, analysing, and presenting digital evidence.
- **Digital Forensics challenges**
  - Cloud computing and IoT have introduced new challenges in accessing and preserving evidence, and dealing with the massive scale of devices.
- **Intersection of Digital Forensics and Incident Response**
  - Digital forensics and incident response work together to investigate, contain, and remediate cyber incidents, with forensics focusing on evidence collection and analysis, and incident response managing the broader recovery process.
- **Essential characteristics to be successful in DFIR**
  - Technical expertise, attention to detail, problem-solving, communication, and the ability to stay calm under pressure.

and much more!

What is Digital Forensics?



Digital forensics is crucial for investigating cybercrime, data breaches, and security incidents in today's digital age by identifying, preserving, analysing, and presenting digital evidence.

Identifying and preserving evidence, documenting findings, and presenting results in court if necessary is part of the process of digital forensics and incident response.

Digital Forensics Challenges

Cloud computing and Internet of Things (IoT) have introduced new challenges in accessing and preserving evidence, and dealing with the massive scale of devices.

Cloud Computing

Cloud Computing is the delivery of computing services such as servers, storage, databases, networking, software, analytics, and intelligence over the internet, or the "cloud".
Cloud services are more flexible, dynamic, and cost effective due to not requiring physical hardware, are scalable to needs, and provide increased accessibility and opportunities for collaboration.

Internet of Things (IoT)

Due to the modernisation of the Operational Technology environment and its convergence with IT, it has created a security threat for organisations to further secure their IT devices to avoid them impacting their OT systems.

The technologies and environments in which vulnerabilities are found have evolved, and thus the landscape of vulnerabilities has evolved, particularly with the rise of cloud computing and generative AI.

External Risks & Cybercriminals

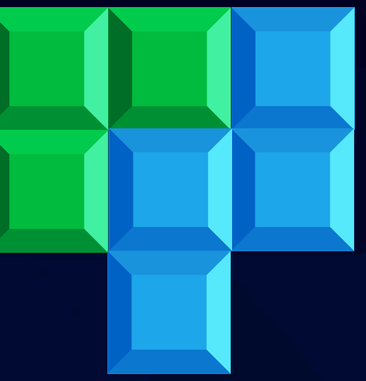
Cybercriminals have embraced the malicious use of AI as these tools can be used to **significantly increase** the sophistication of social engineering attacks and other email threats, with no technical knowledge required.

Cybercriminals are drawn to the:

- Low barrier to entry for generative AI tools.
- Ability to rapidly create high volumes of malicious content.
- Increased sophistication of existing attacks (phishing, vishing, smishing, etc).
- Little technical understanding required.

The technologies and environments in which vulnerabilities are found have evolved, and thus the landscape of vulnerabilities has evolved, particularly with the rise of cloud computing and generative AI.

Intersection of Digital Forensics and Incident Response



Digital forensics and incident response work together to investigate, contain, and remediate cyber incidents.

Forensics focuses on **evidence collection and analysis**.

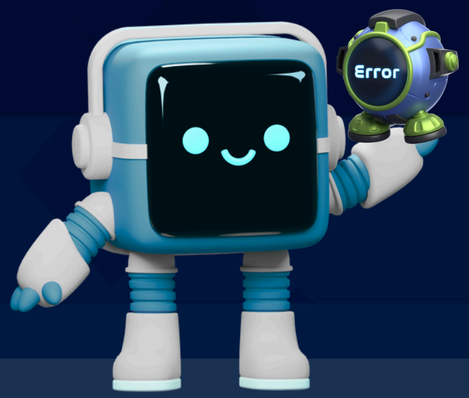
Incident response is focused on managing the **broader recovery process**.

Continuous training is vital to keep up with the evolving technology. Digital Forensics investigators must be adaptable, often becoming experts in new technologies quickly due to the ever-changing nature of cyber security.

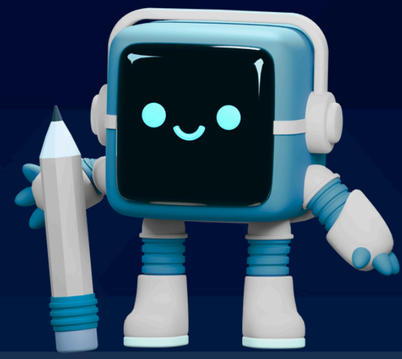
Common Incidents

Common incidents requiring both digital forensics and incident response include malware outbreaks, data breaches, insider threats, and nation-state attacks.

- Continuous training is vital to keep up with the evolving technology.



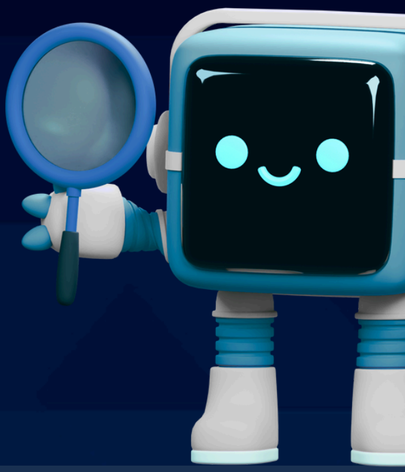
- Must be adaptable, often becoming experts in new technologies quickly.



Staying up-to-date in the field of DFIR requires continuous learning, attending conferences, collaborating with peers, and experimenting with new tools and techniques.

Essential Skills for DFIR Staff

- Love of the deeply technical - how things work
- Attention to detail - spotting clues and trawling
- Problem-solving - solving puzzles!
- Communication - sharing knowledge and collaborating
- Remaining calm under pressure - high stress environments



"A good investigator is like a hunting dog. You let them go and they will go and go and go hunt until they either get what they're hunting for or you call them back, right. And they just will not relent." - Nick Klein

Security Maturity & Organisational Readiness

Organisational readiness for pen testing, including the staged approach from blue teams to red teams, highlights the importance of maturity in cyber security practices.

The Essential 8 Maturity Model

The purpose of the Essential 8 Maturity Framework is to provide organisations with a baseline of eight essential mitigation strategies to help protect their systems against cyber threats. The framework provides guidance on protecting Windows networks.

Maturity Model assessments should be conducted based on the organisation's current and desired level of maturity.

Achieving higher maturity levels requires continuous improvement, monitoring, and adaptation to the evolving threat landscape.

Organisational readiness for pen testing, including the staged approach from blue teams to red teams, highlights the importance of maturity in cyber security practices.

Phriendly Phishing

PODCASTS

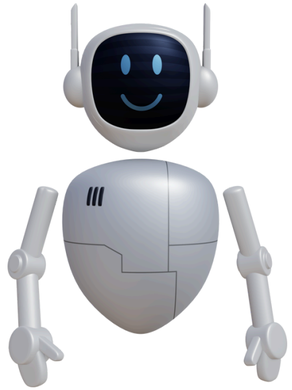
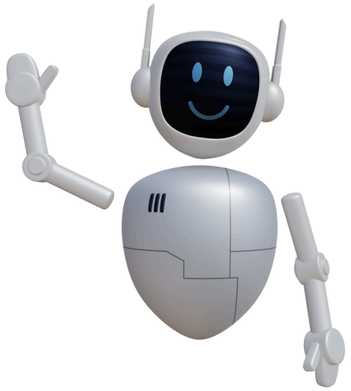
www.phriendlyphishing.com

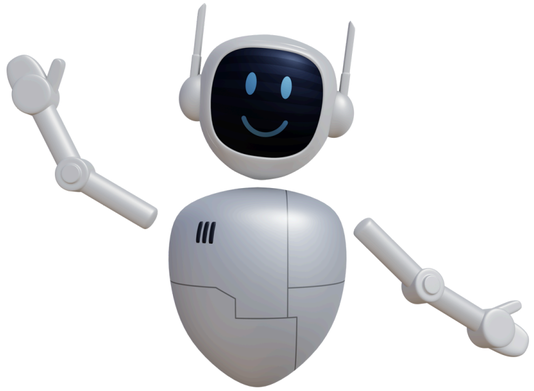
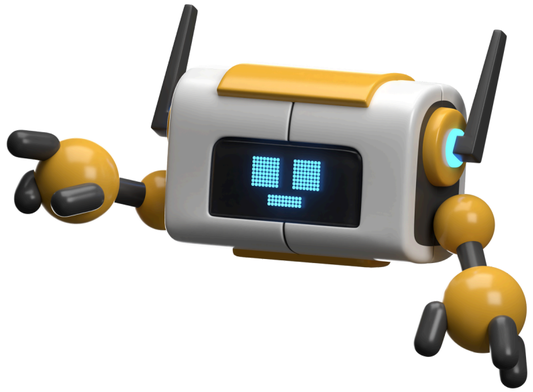
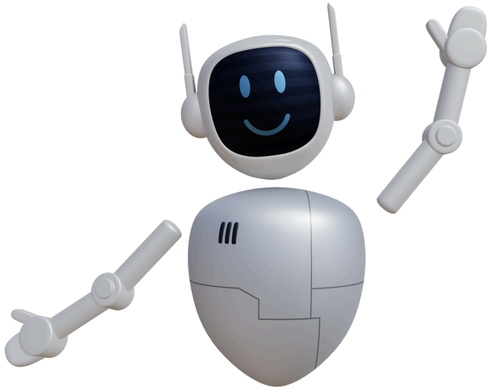
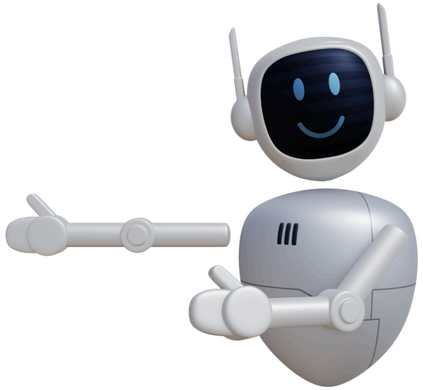
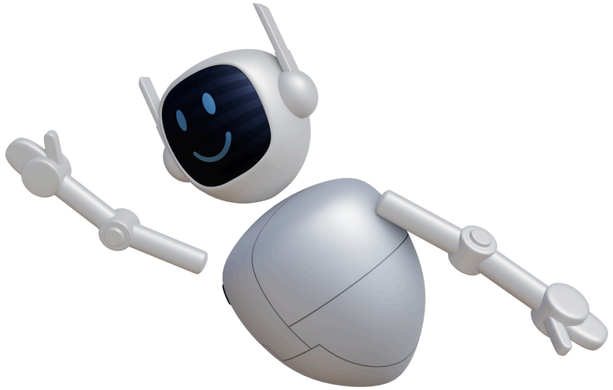
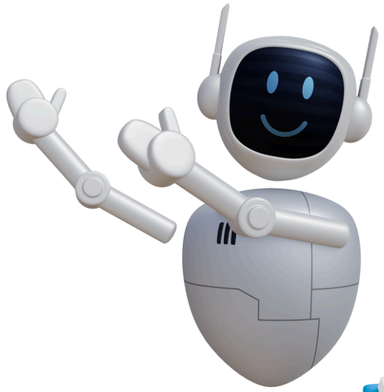
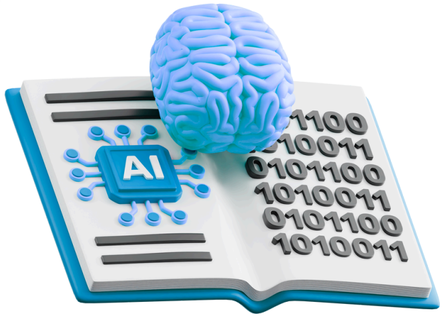
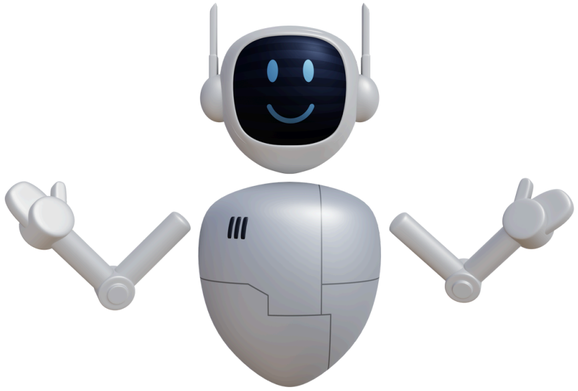
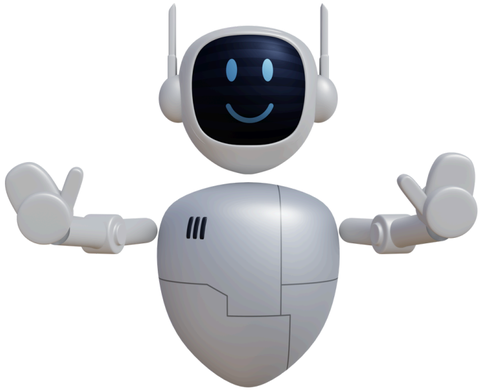
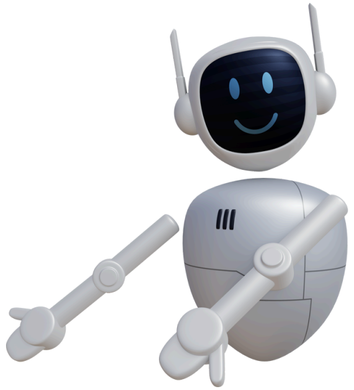
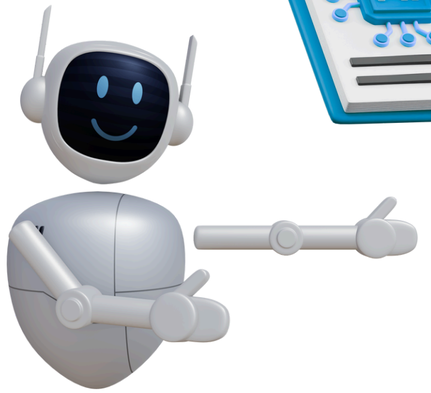
Stay tuned for more!

BYTES

WITH BEC & BENJI

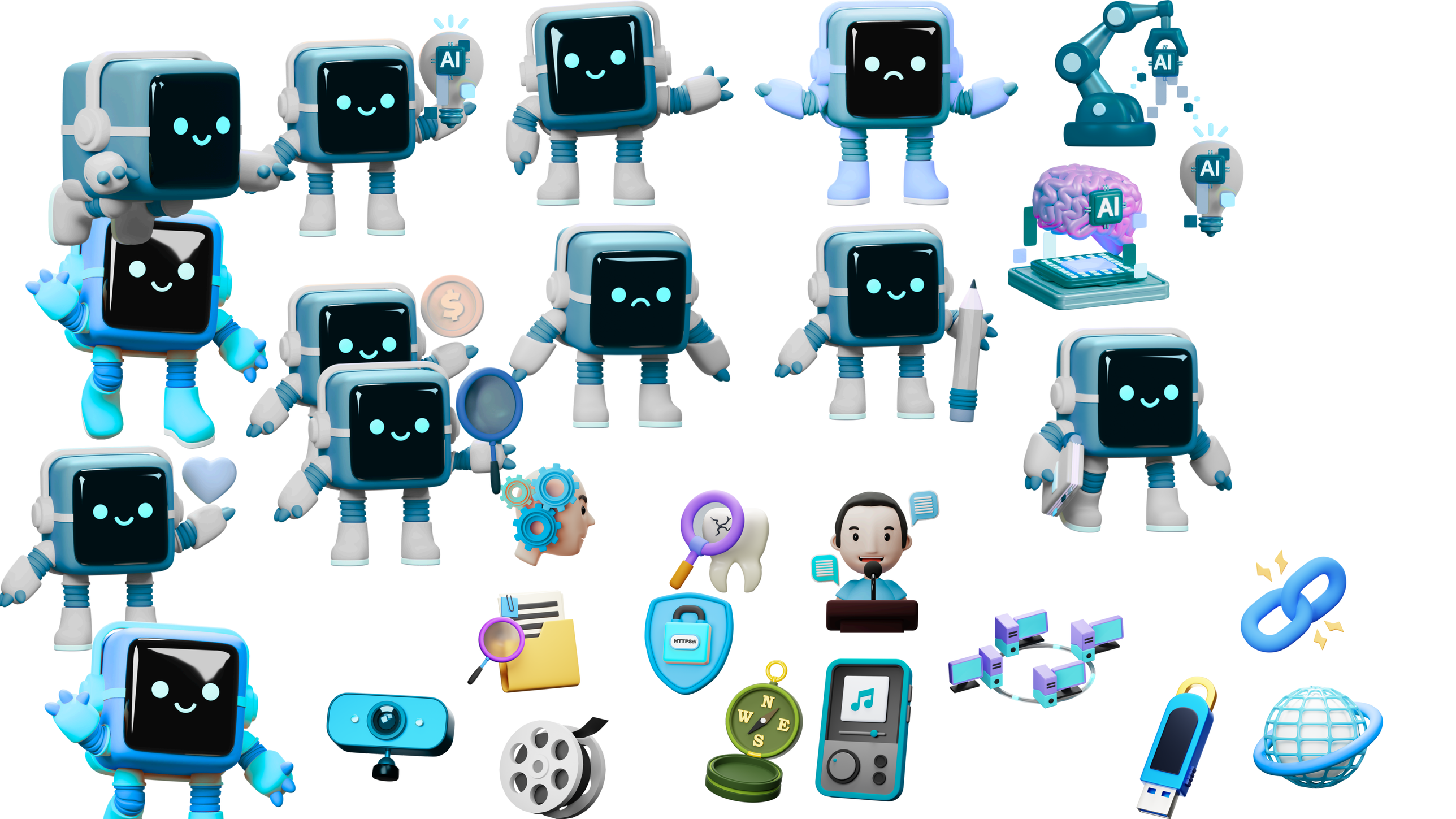
https://linktr.ee/BytesBB

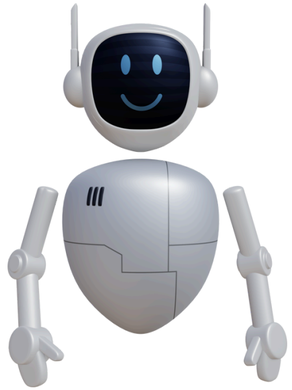
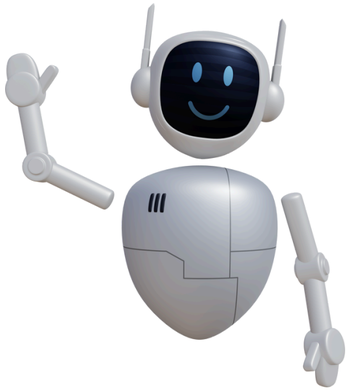



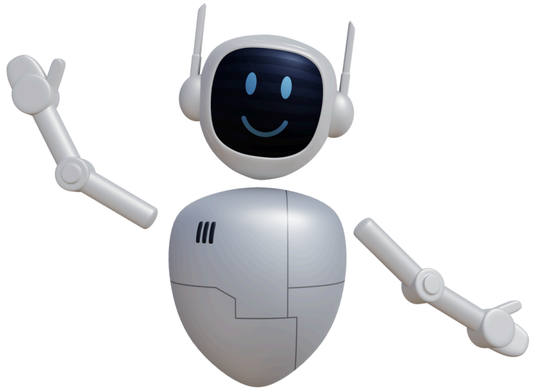
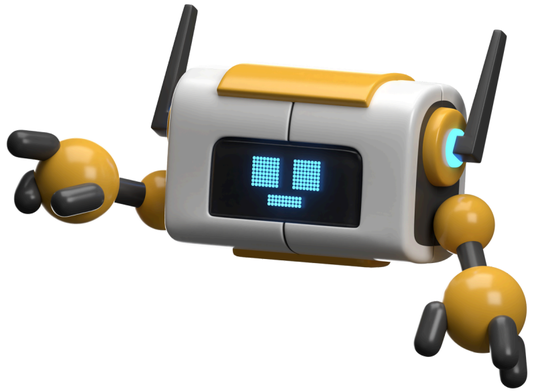
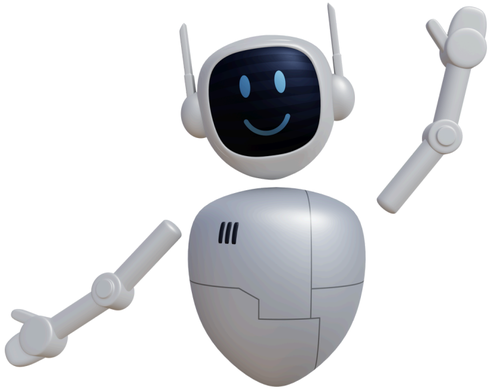
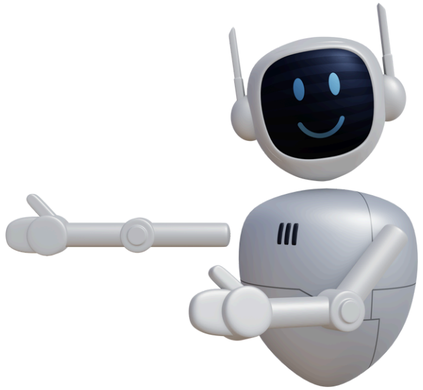
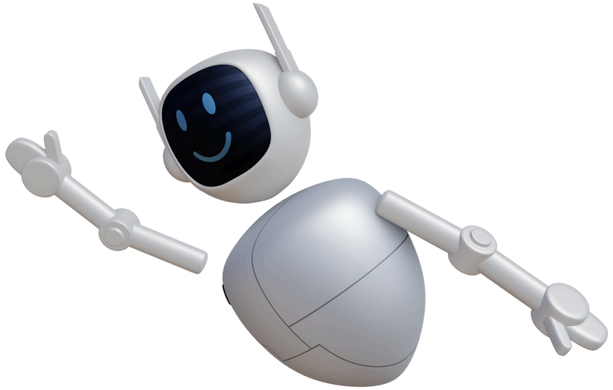
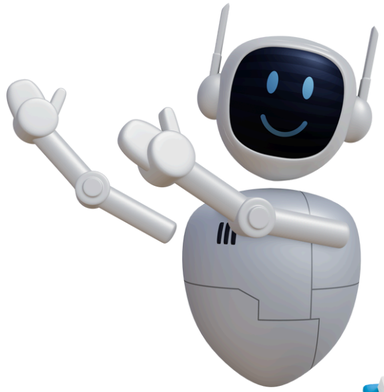
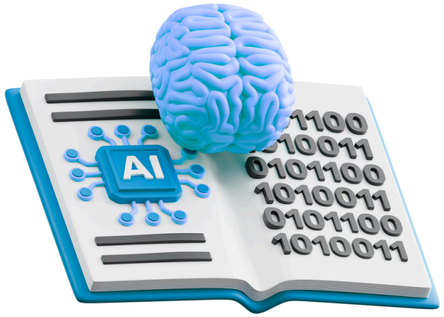
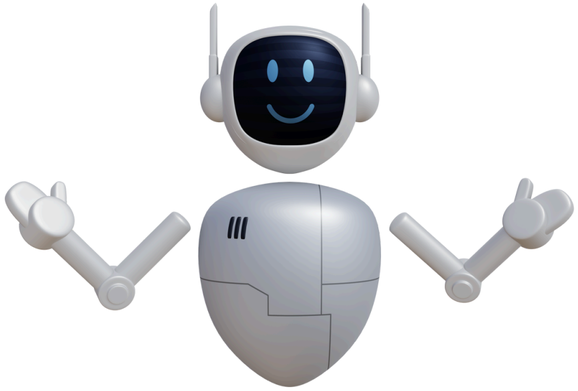
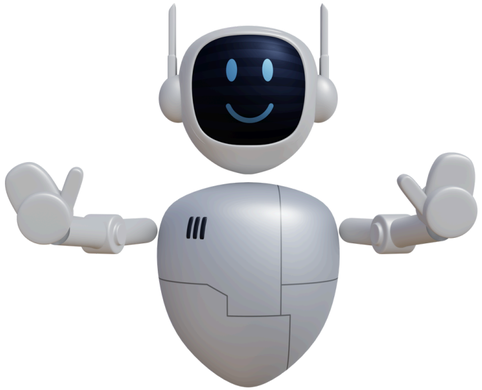
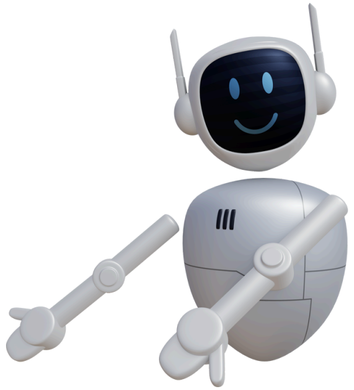
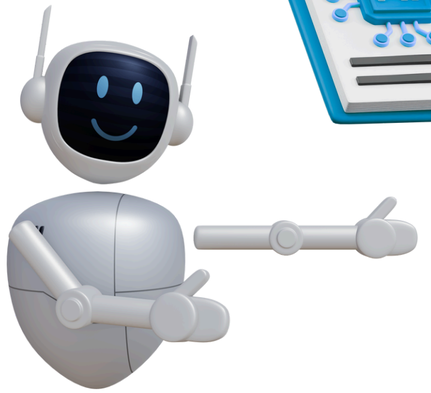







AI
1100
10011
0101100
1010011
0101100
1010011






Error
75%


0011
0110
Hello

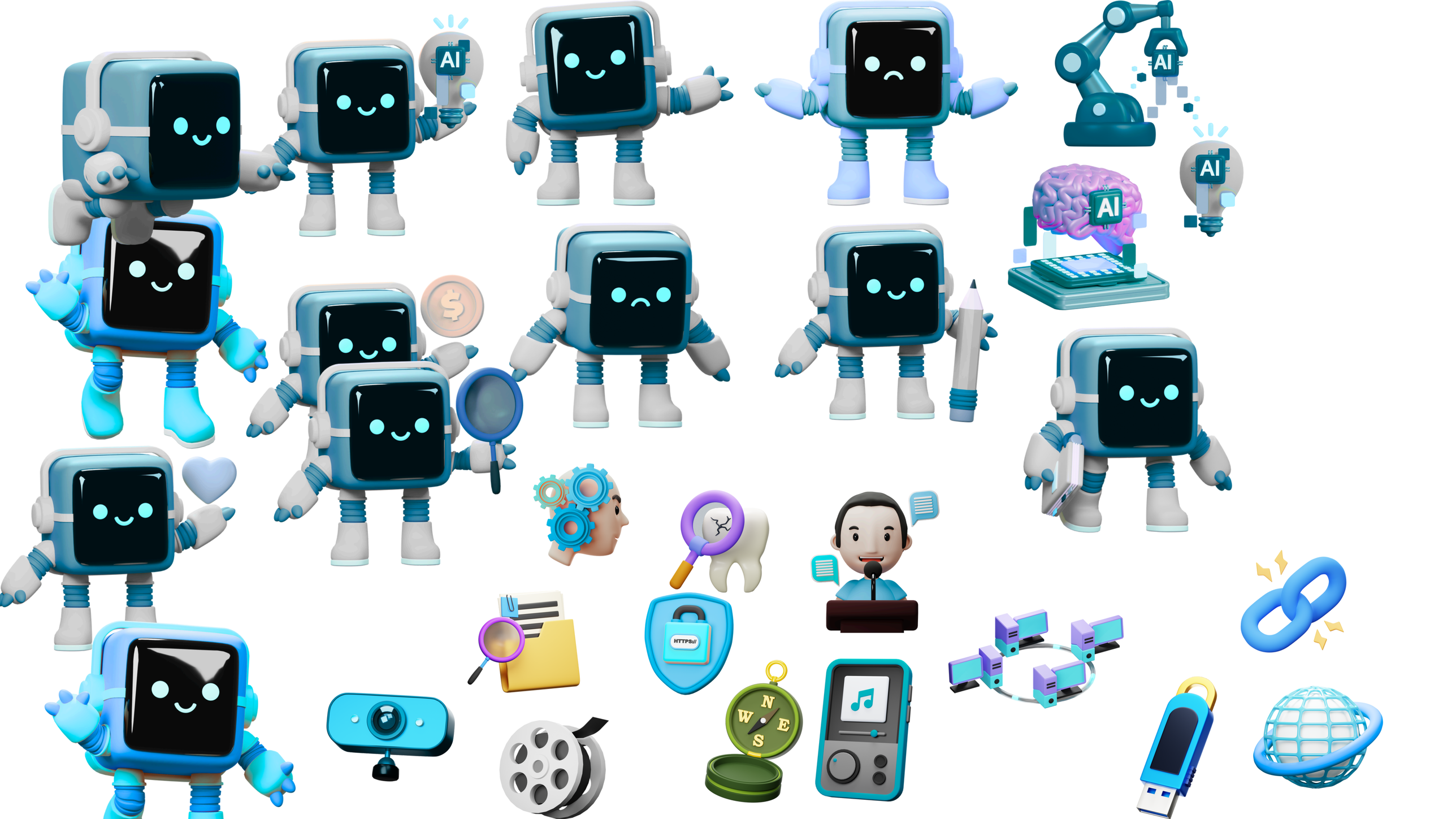

AI
AI
AI
AI
HTTPS://
N
W
E
S








AI
1100
10011
0101100
1010011
0101100
1010011






Error
75%


0011
0110
Hello


AI
AI
AI
AI
HTTPS://
N
W
E
S