



HKCERT

Hong Kong Computer
Emergency Response Team
Coordination Centre
香港電腦保安事故協調中心

Cyber Security Challenges of Metaverse



Agenda

1. About HKCERT
2. Cybersecurity Challenges of Metaverse
3. Advice



International

Local

Exchange Incidents
and Information

HKCERT as a Hub

Coordinate incidents
and publish alerts

Global
Researchers



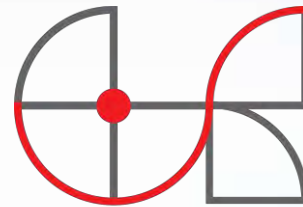
Global CERT Forum

APNIC

DOT ASIA
ORGANISATION



Regional CERT
Forum



HKCERT



GovCERT.HK



Internet
Infrastructure



Regulators



Enterprises



Universities &
Researchers



IT & Security
Vendors

About HKCERT

2001

Founded

100%

Funded by
Government

7 x 24

Operation

4,000+

Incidents Handled
in 2022 H1

200+

Security Advisories
Published in 2022 H1

2M+

People Reached

3,500

People Trained

100%

of cases resolved
within 5 working days

Service and Support by HKCERT



Monitoring

- Collect and Analyse Attack Patterns
- Provide Early Information Security Alerts



Education and Technical Advice

- 24-hours Free Incident Report Hotline (8105-6060)
- Organise Free Seminars and Briefings
- Collaborate with Local Industry, Government Agencies, and Global CERTs



Research and Insights

- Offer Best Practice and Guideline
- Provide Online Cyber Security Self-Assessment Tool

2

Cyber Security Challenges of Metaverse



What is Metaverse

Elements of a Metaverse



gartner.com

Source: Gartner
© 2022 Gartner, Inc. and/or its affiliates. All rights reserved. GTMKT_3635001

Gartner

- “It is a collective virtual space, created by the convergence of virtually enhanced physical and digital reality. In other words, it is device-independent and is not owned by a single vendor. It is an independent virtual economy, enabled by **digital currencies and nonfungible tokens (NFTs)**.
- A Metaverse represents a combinatorial innovation, as it requires multiple technologies and trends to function. Contributing tech capabilities include **augmented reality (AR)**, flexible work styles, **head-mounted displays (HMDs)**, an AR cloud, the Internet of Things (IoT), 5G, **artificial intelligence (AI)** and spatial technologies.” - **Gartner**

Security Risks of Metaverse

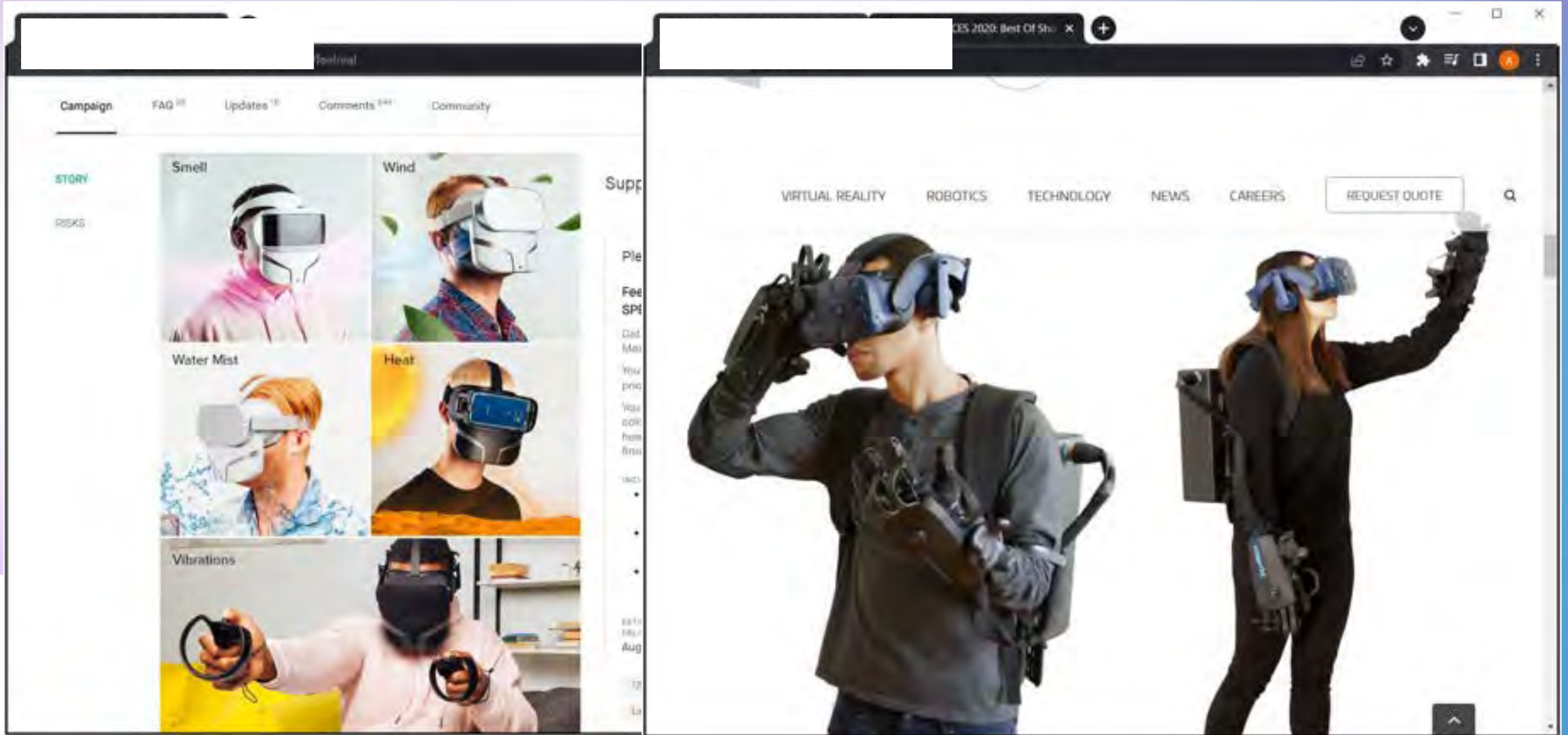
Security Risks of Metaverse

- **Vulnerabilities of AR/VR devices**
- **Identity and Authentication**
- **NFT and Smart Contract**
- **Decentralisation vs Regulation**

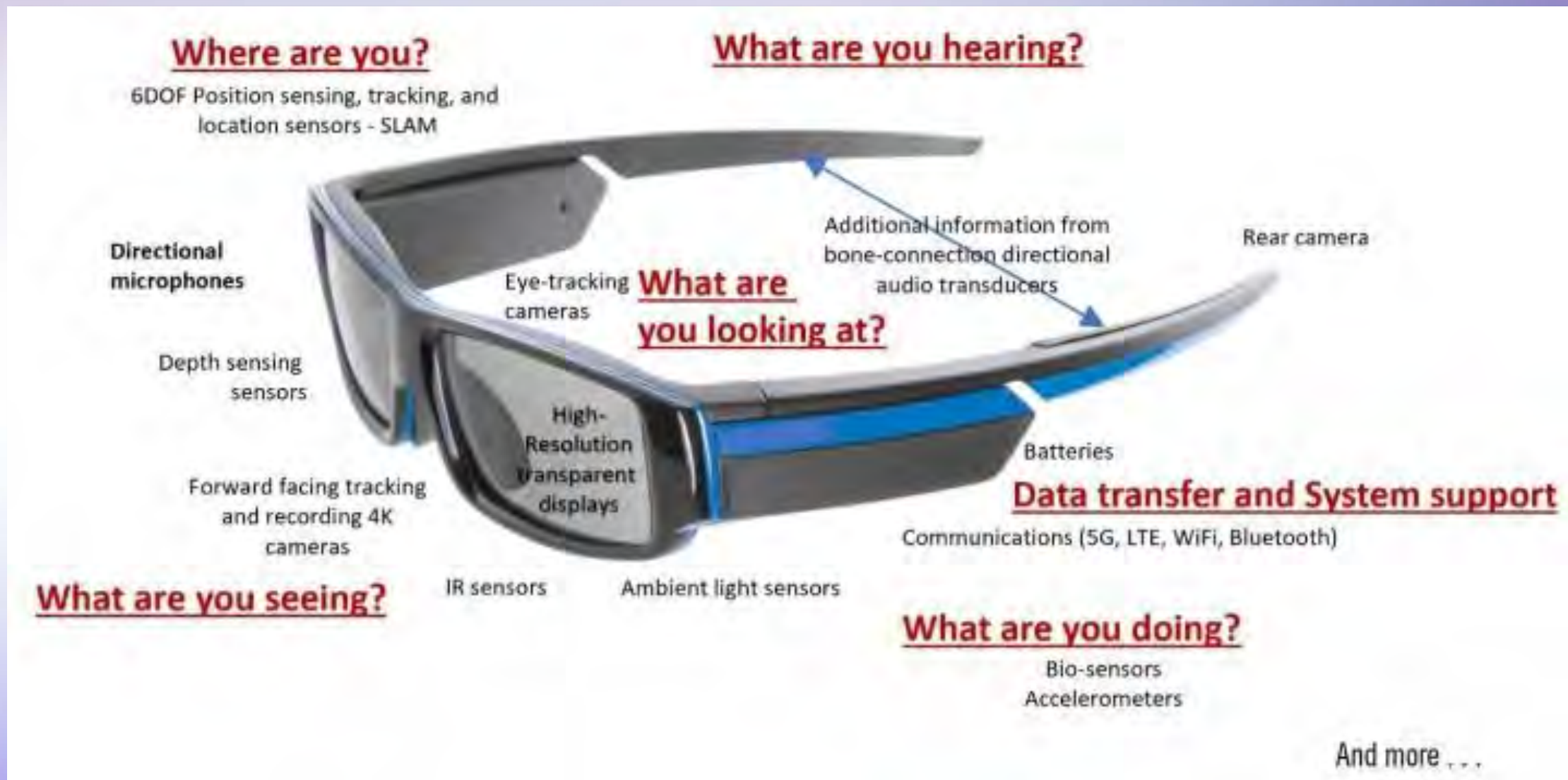
Security Concerns of AR/VR devices

	Augmented Reality (AR)	Virtual Reality (VR)
Definition	<ul style="list-style-type: none">Enhances or ‘augments’ the real world by adding digital elements – visual, auditory, or sensory – to a real-world view.Example: Pokémon Go, Google Glass / AR	<ul style="list-style-type: none">Creates its own cyber environment.Usually experienced through an interface, such as a headset or goggles (i.e. immersive)
Top risks	<ul style="list-style-type: none">Privacy (e.g. eye, finger, motion tracking, biometrics)Data Security (e.g. inbound / outbound encryption)<u>Malware</u> & Ransomware (e.g. VR malware that lets hackers record your headset screen, collect data, corrupt work instructions or disrupt operation)Unreliable content – misleading or false information	

Data Privacy: Multi-sensory Devices

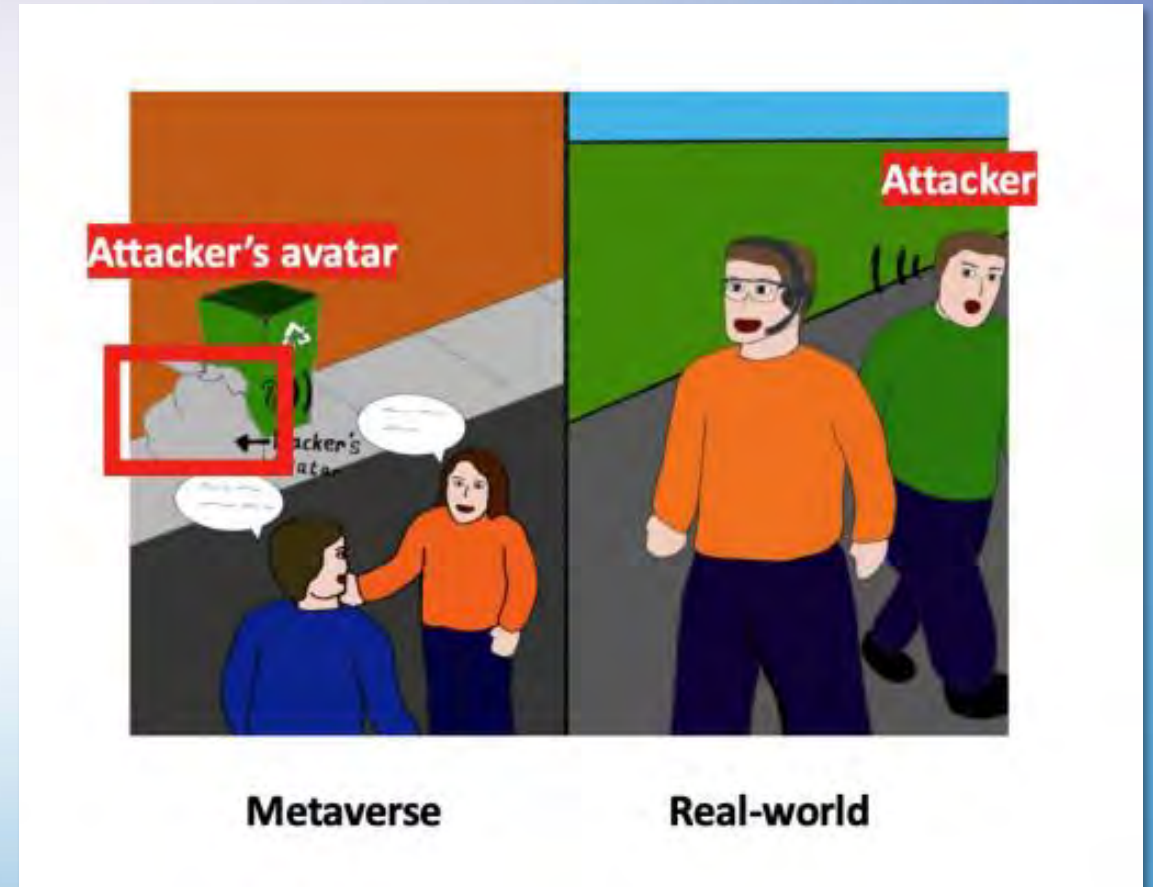


Data Privacy: Multi-sensory Devices



Identity Issue in Metaverse

- In the metaverse, individuals can create **virtual avatars**:
 - **Realistic** following the real individual characteristics (e.g., age, gender)
 - **Fictional**, an animal or other person:
 - ❑ Or use **deep-fakes** to generate a similar person to confuse other avatars
- Attackers can use such **avatars to blend in the virtual world**, as the example on the right, where the attacker is a **trash bag eavesdropping other avatars' conversations**



Fake Identities and DeepFake



Fake Identities and DeepFake



***Guess which
person is
real?***

Fake Identities and DeepFake



Answer: All are synthesized by AI

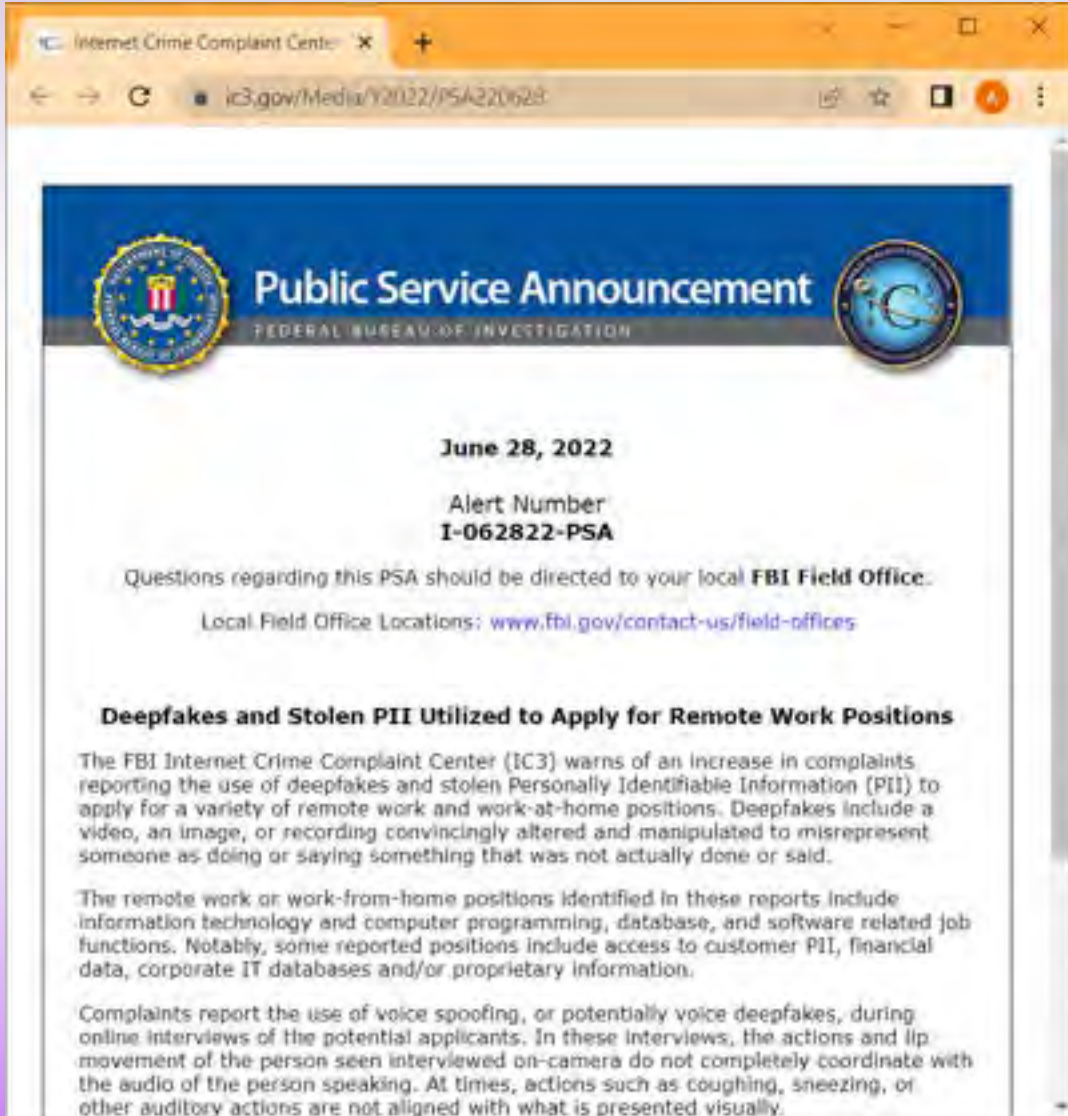
<https://www.thispersondoesnotexist.com/>

Fake Identities - Voice Phishing or “Vishing”



- Criminal case happened in 2019
- CEO of a UK based energy firm transferred **US\$243,000** to a fraudster
- The criminal used artificial intelligence-based software to impersonate the voice of chief executive of the firm's German parent company with German accent

Fake Identities - Zoom Phishing or “Zishing”



- In 2022 June, FBI issue warning of cybercriminals using Americans' stolen Personally Identifiable Information (PII) and deepfakes to apply for remote work positions.
- Through online interviews with convincingly altered videos or images.
- Target positions in the tech field that would allow the malicious actors to gain access to company and customer confidential information after being hired.

Digital Identity

Digital identity is enabling decentralization and new forms of verification – examples of innovation

	Self-sovereign identity (SSI)	'Passwordless' identity
Diagram		
Description	<ul style="list-style-type: none"> Users have control over their verified credentials (attribute information to identify an individual); they can select the specific data for sharing (eg, name, password) and the sharing audience (eg, employers, healthcare provider) 	<ul style="list-style-type: none"> Users can verify and authenticate their digital identity without traditional alphanumeric passwords but with other forms of identifying information
Functionality	<ul style="list-style-type: none"> Users interact directly with ID issuers and organizations without relying on an intermediary to facilitate data exchange Data and user credentials are stored on a decentralized ledger (eg, blockchain) for easy access and verification 	<ul style="list-style-type: none"> Users can provide alternative identifying information, such as: <ul style="list-style-type: none"> Biometrics (eg, facial scan, retinal scan, thumbprint, voice) Devices and apps (eg, mobile phone, email) Documents (eg, driver's license, passport)
Benefits	 <ul style="list-style-type: none"> Increased individual control over identity for trusted transactions without an intermediary; users themselves control what data they share and with whom from an interoperable and convenient identity source Improved security, because decentralized data storage limits vulnerability to attacks 	<ul style="list-style-type: none"> Alternative protections against rising vulnerability attacks (eg, phishing, brute-force password cracking) Reduced inefficiencies for the user (eg, too many passwords, lost password) Efficiency and convenience; users can rely on streamlined identifying information, based on the level of risk associated with the system

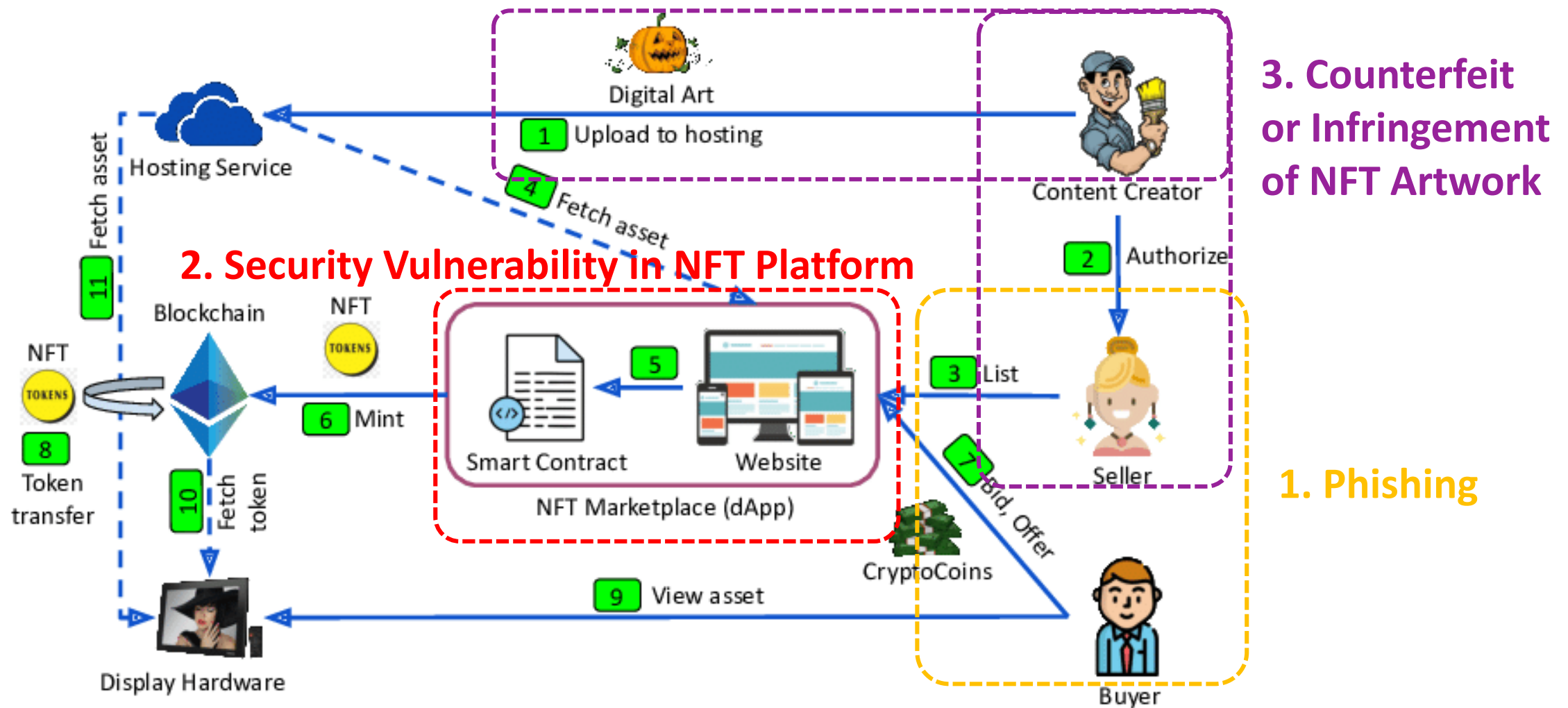
¹Diagram adapted from Alex Brown, "Passwordless authentication: A complete guide [2022]," Transmit Security, Jan 13, 2022.

Source: Expert input; McKinsey analysis

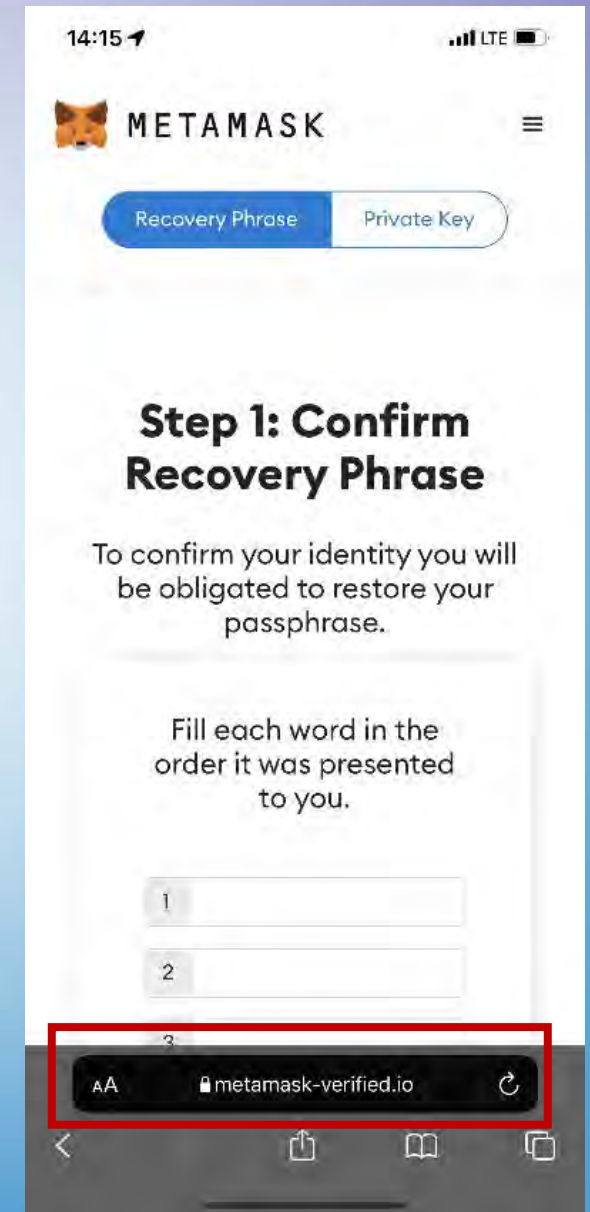
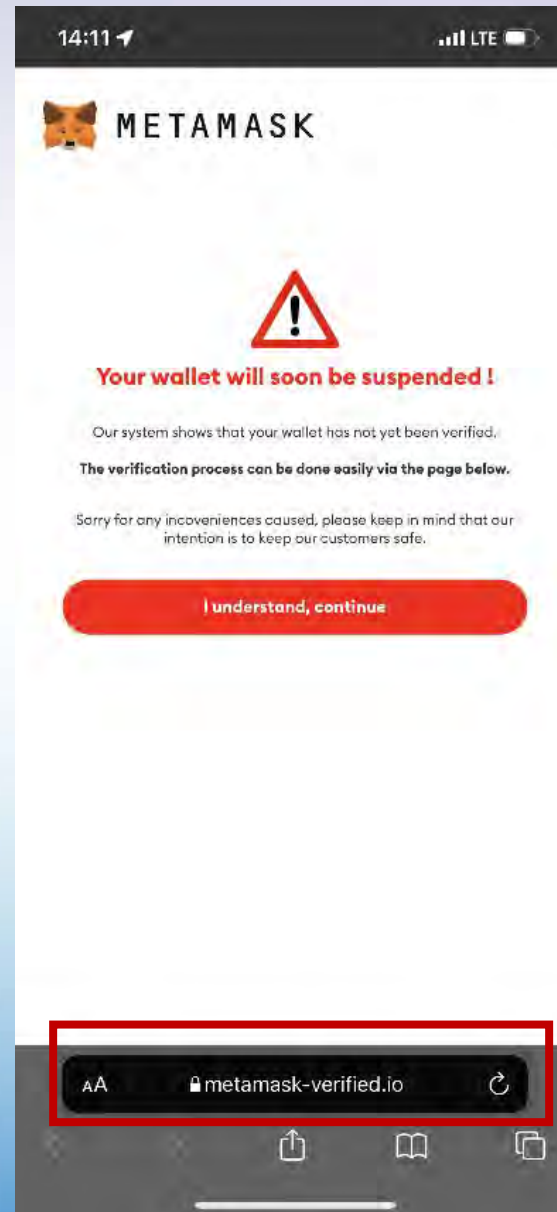
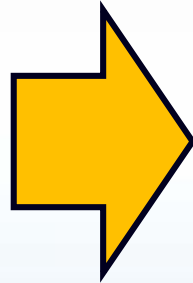
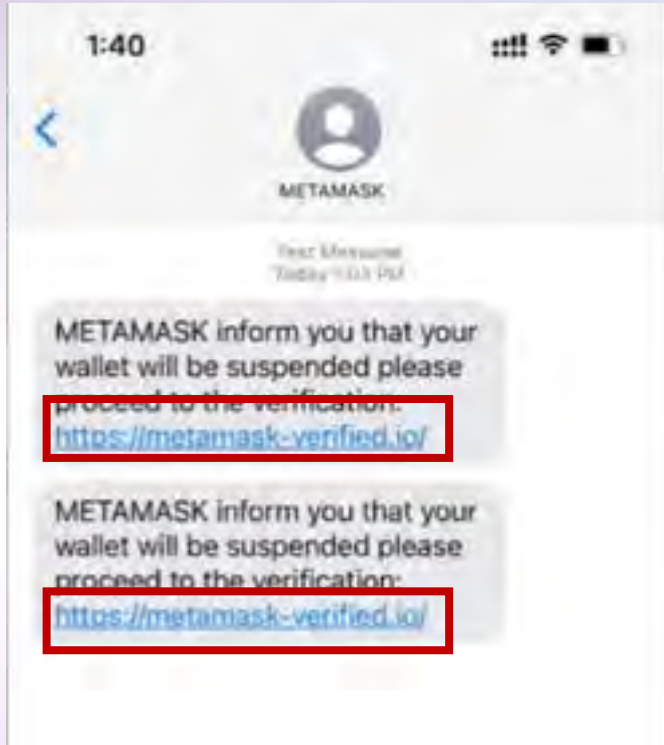
McKinsey & Company

6

Security Issues in the NFT Ecosystem



1) NFT - Phishing



Fake <https://metamask-verified.io/>

Real <https://metamask.io/>

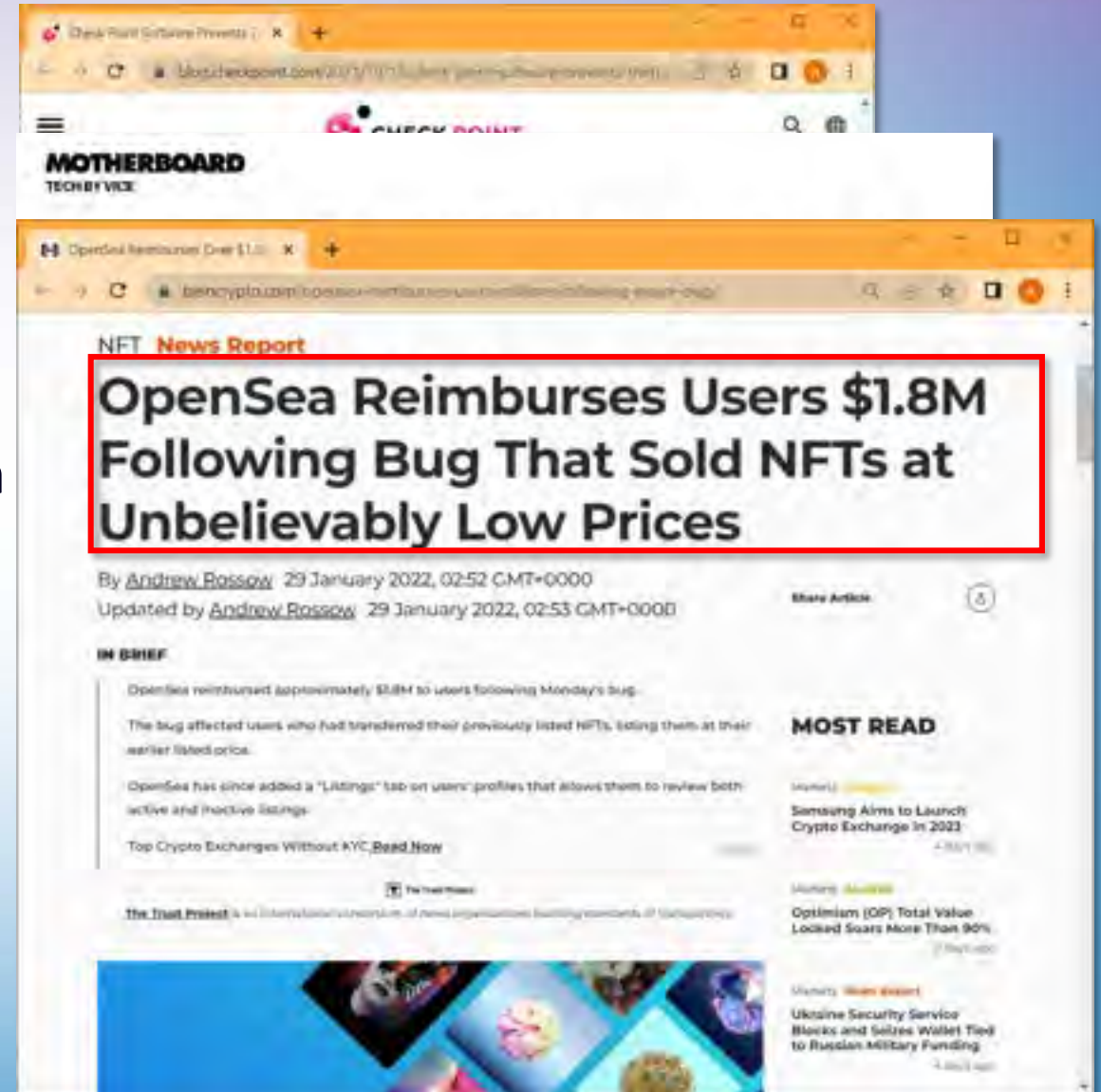
2) NFT – Platform Vulnerabilities

Insufficient security consideration during the design and development phrases

- Allow to upload artworks containing malicious code (e.g. SVG)
- Lack of MFA/2FA support in the platform
- Platform design flaws

Impact

- Asset stolen
- User accounts compromised
- Bad actors bought NFTs at low prices from owners



Security Risks of Cryptocurrency

Cryptocurrency

“Hot wallet”

- Requires an internet connection
- Vulnerable to **cyber attacks** or **data breach**



“Cold wallet”

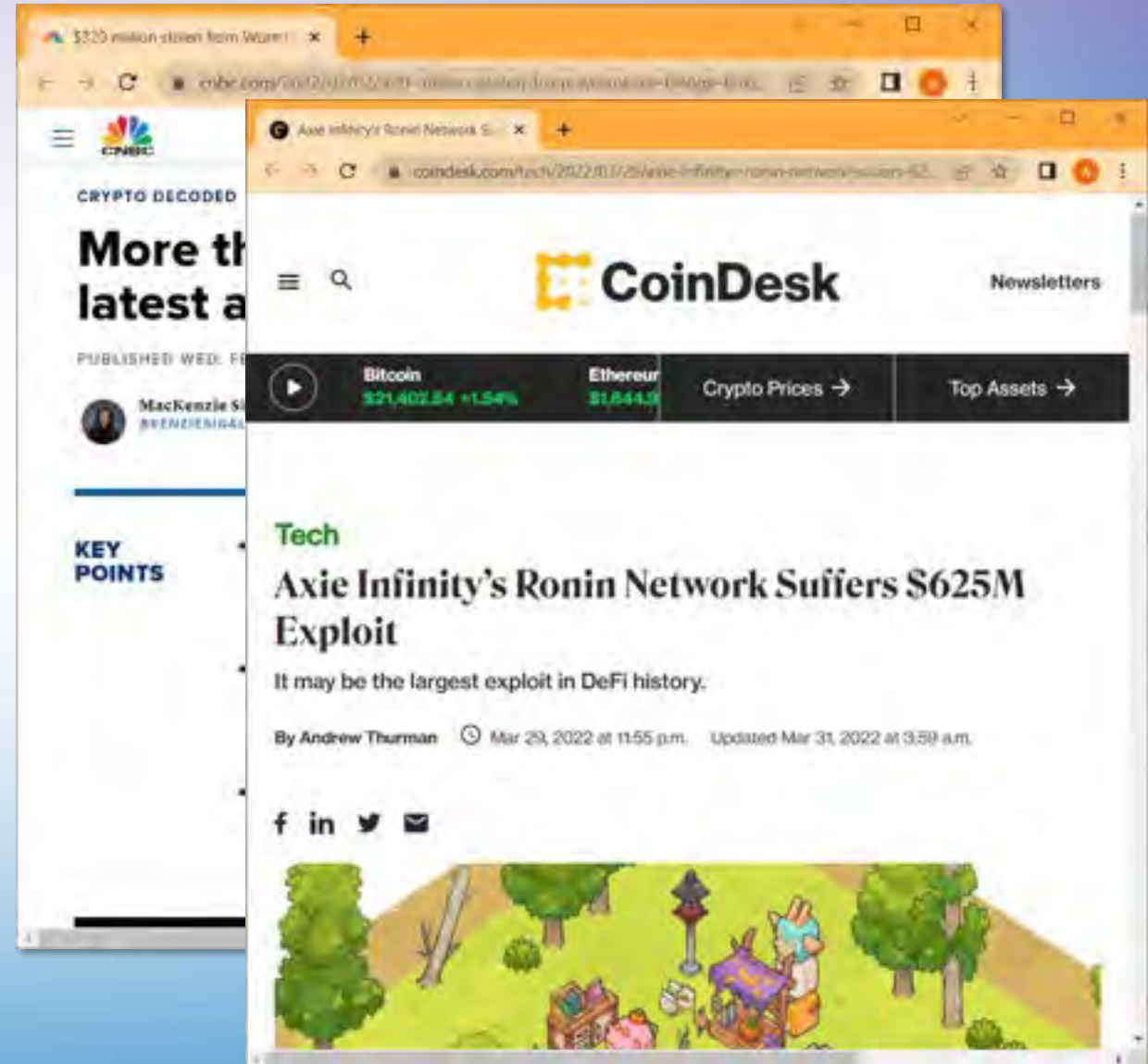
- Does NOT require an internet connection
- At risk of **physical loss or damage**, **storage device malfunction**



Security Issues in Smart Contract



- The **smart contract** is **programmed** and written into the **blockchain**, which **cannot be tampered** with.
- Also, once the conditions defined are met, the content will be **executed immediately and automatically**.
- Many security incidents are caused by hackers **finding vulnerability in the programs**.



Security Issues in Smart Contract

TRADITIONAL CONTRACT



SMART CONTRACT



Recommendations:

- Review **the contract content carefully** when signing.
- If not too familiar with smart contracts, use the **official smart contracts** on the trading platform
- After the transaction, check the **crypto asset immediately**
- When **writing smart contracts**, refer to the **best practice guidelines** to avoid common attack methods, such as re-entrancy, denial of service attacks, etc.
- Conduct **security assessment or auditing against smart contracts to examine the code**

Decentralisation vs Regulation

Virtual Asset

- **Virtual assets** should be regarded as “**objects**” that can be “**stolen**”?
- Or **access to computer** with criminal or dishonest intent **under criminal law**?
- **Cross-border issues** may arise?
- Will the **transfers of NFTs** constitute **taxable** transactions?

“Ownership” of Lands

- **Smart contract** templates provided by the transaction platform is **very simple form**, merely contain **monetary obligations** and term limitations.
- Necessary to improve the **legal protection to the owners** of the land in the metaverse

Payment

- By agreeing to complete the transaction of bitcoins, the parties involved **automatically accept the terms and conditions** provided by such platform
- Possible to have a **universal law** to **regulate** all payment disputes in this virtual world?
- If doing so, does it simply frustrate the **decentralised concept** of blockchain technologies?

3

Advice



Information Security Advice (Corporate Level)

1

Formulate Strategies & Develop Relevant Security Measures to Tackle New Security Risks

- **Cryptocurrency, Metaverse and Emerging Technologies**

2

Monitor Third-Party Security Risks to Tackle Supply Chain Attacks and Improve Security Defence Mechanism

- Vendors and software applications (e.g., Log4j)

3

Conduct Regular Security Health Check on Network and System

- Monitor IT assets connected to internet continuously

Information Security Advice (Individual Level)

1

Enable Multi-factor Authentication and Asset Transfer Whitelist to Protect Personal Crypto Assets (e.g., NFT)

2

Turn Off QR Code Scanner's Automatic URL Redirection Function to Prevent QR Code Attacks

- Do not scan QR Codes from **unknown sources**

3

Pay Attention to the Spelling of Domain Names of Websites to Avoid Phishing Websites

- Check the **authenticity** of websites

Subscription to HKCERT Information Security Alert Service

To stay vigilant against **information security risks**, please subscribe or follow:

1. Free Security Bulletin and Monthly Newsletter



2. Free SMS Alert



3. HKCERT's Social Media Platforms (e.g., Facebook, LinkedIn and YouTube)



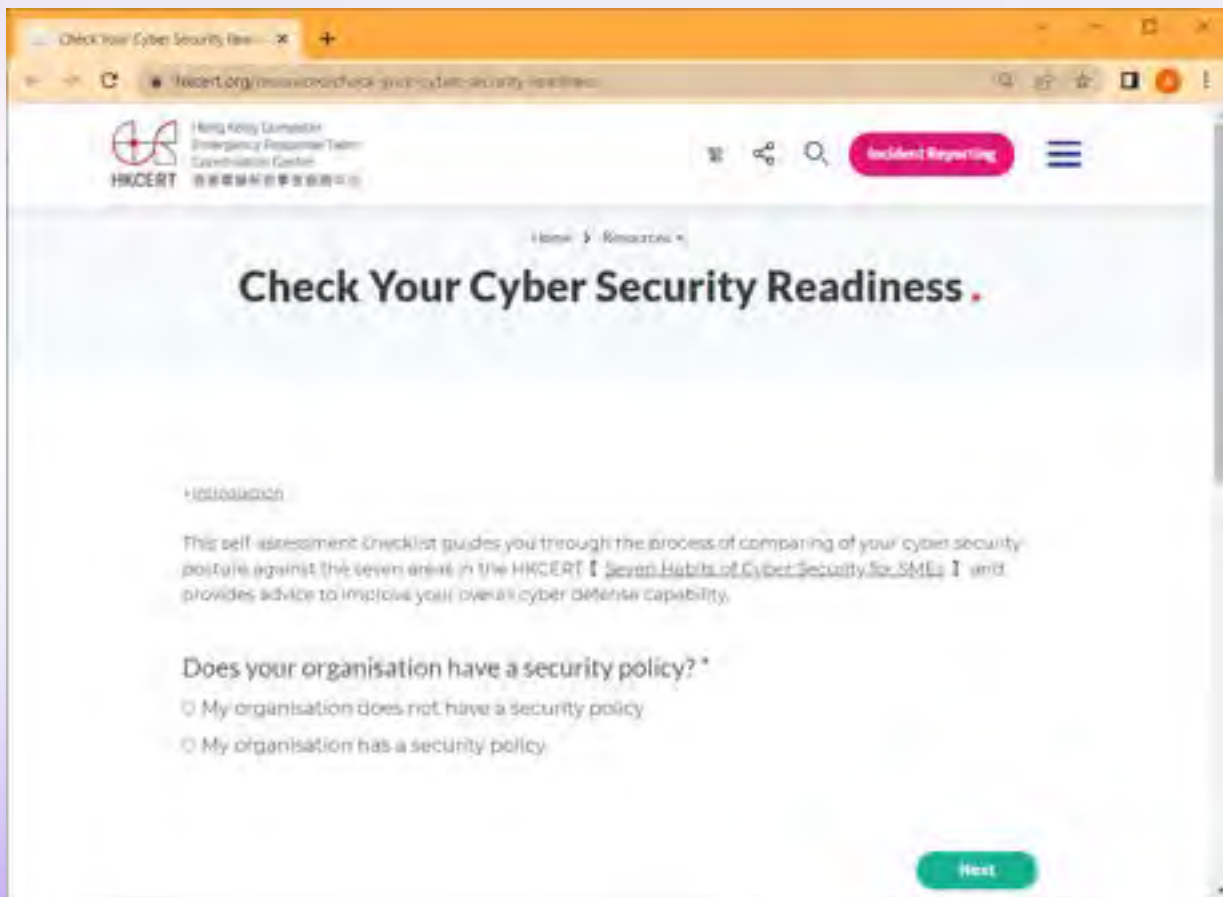
Take Action Now!

<https://www.hkcert.org/tc/form/subscribe/entry>

SUBSCRIBE



Online Self Assessment & Incident Response Guideline for SMEs



The screenshot shows a web browser window with the URL <https://www.hkcert.org/online/self-check-your-cyber-security-readiness>. The page features the HKCERT logo and navigation links. The main heading is "Check Your Cyber Security Readiness". Below this, there is an "Introduction" section stating: "This self-assessment checklist guides you through the process of comparing of your cyber security posture against the seven areas in the HKCERT [Seven Habits of Cyber Security for SMEs] and provides advice to improve your overall cyber defense capability." A question is posed: "Does your organisation have a security policy? *". Two radio button options are provided:
☐ My organisation does not have a security policy
☐ My organisation has a security policy
A green "Next" button is located at the bottom right of the form.





將於11月11-13日舉行，設有中學組，大專組及公開組，設有**豐富獎品**

立即於**10月31日**前報名，10月中更會有工作坊講解備戰方法

👉 <https://ctf.hkcert.org> 🔍



比賽方式

網上比賽以解題模式奪分，成功解題後可以獲得一套**特定字串**，而該特定字串在CTF世界中叫「旗」，組內頭三隊最高分便為贏家

題目

- 程式漏洞
- 密碼學
- 網絡鑑證
- 逆向工程
- 網站保安



Hong Kong Productivity Council 香港生產力促進局

HKPC Building, 78 Tat Chee Avenue, Kowloon, Hong Kong
香港九龍達之路78號生產力大樓
+852 2788 5678 www.hkpc.org

