Bulletin of May 2025

Cybersecurity Bulletin

Risks of using company account log-in to unauthorized devices

Unauthorized devices such as **'Personal computer'** may not have **adequate security**, increasing the risk of compromise or unauthorized access due to **limited advanced detection**.

Example scenario :

1-Logging In on unauthorized device

You use your personal computer to access your company OneDrive.

2-Malware on unauthorized device

Unfortunately, your personal computer has a hidden program (malware) that steals information.

3-Your Login Details Stolen

This malware secretly copies your OneDrive username and password.

4-Your Credentials in the Wrong Hands

The stolen username & password is sent to attacker.

Example of Cybercrimes attacker commit by leveraging from stolen username & password :

- **Lateral Movement**

In a corporate environment, attackers use compromised employee credentials to **move laterally through the network**, **gaining access to more sensitive systems and data**. This can lead to significant data breaches, intellectual property theft, or disruption of operations.

- **Ransomware Attacks**

Attackers may use stolen credentials to **gain access to critical systems** and deploy ransomware, encrypting data and demanding payment for its release.

"Secure company account as if it were your personal ID"

DO	DON'T
Use company system account/e-mail account with ***authorized devices*** only. *(such as company device, Device registered with company)*	Use company system account/e-mail account with ***unauthorized device***. *(such as personal device, device not registered with company)*

Source: Toyota Asia Cybersecurity Team

Cybersecurity Bulletin

ความเสี่ยงจากการใช้บัญชีของบริษัทกับอุปกรณ์ที่ไม่ได้รับอนุญาต

อุปกรณ์ที่ไม่ได้รับอนุญาต เช่น 'คอมพิวเตอร์ส่วนตัว' อาจ**ไม่มีความปลอดภัยเพียงพอ** ทำให้มีความเสี่ยงต่อการถูกเจาะระบบหรือการเข้าถึงอุปกรณ์และข้อมูลโดยไม่ได้รับอนุญาต

ตัวอย่างสถานการณ์ :

1-การเข้าสู่ระบบของบริษัทผ่านทางอุปกรณ์ที่ไม่ได้รับอนุญาต	2-มีมัลแวร์แฝงในอุปกรณ์	3-ข้อมูลถูกโจรกรรม	4-ข้อมูลของคุณตกไปอยู่ในมือผู้โจมตี
พนักงานใช้คอมพิวเตอร์ส่วนตัวเพื่อเข้าถึง OneDrive ของบริษัท	คอมพิวเตอร์ส่วนตัวของคุณอาจมีมัลแวร์แฝงตัวอยู่ มัลแวร์เหล่านี้สามารถเข้าถึงข้อมูลในอุปกรณ์ได้	มัลแวร์จะแอบคัดลอกชื่อผู้ใช้และรหัสผ่าน OneDrive ของคุณโดยที่คุณไม่รู้ตัว	**ชื่อ**ผู้ใช้และรหัสผ่านที่ถูกคัดลอกจะถูกส่งไปที่แฮ็กเกอร์

ผู้โจมตีใช้ประโยชน์จากชื่อผู้ใช้และรหัสผ่านที่โจรกรรมมาอย่างไร :

- **การเคลื่อนที่ภายในระบบเครือข่าย**

ผู้โจมตีมักใช้บัญชีของพนักงานที่ถูกโจรกรรมไป เพื่อทำการเจาะระบบ จากนั้นจะค่อยๆ**เคลื่อนที่ภายในเครือข่ายไปยังระบบอื่น ๆ เพื่อเข้าถึงข้อมูลหรือระบบที่มีความสำคัญ** ซึ่งอาจนำไปสู่การรั่วไหลของข้อมูลครั้งใหญ่ การโจรกรรมทรัพย์สินทางปัญญา หรือทำให้การดำเนินงานขององค์กรหยุดชะงัก

- **การโจมตีด้วยซอฟท์แวร์เรียกค่าไถ่**

ผู้โจมตีจะใช้**ชื่อผู้ใช้และรหัสผ่าน**ที่โจรกรรมมา เพื่อเข้าถึงระบบที่สำคัญขององค์กรแล้วติดตั้งซอฟท์แวร์เรียกค่าไถ่ (Ransomware) ทำการเข้ารหัสข้อมูลทั้งหมด และเรียกค่าไถ่เพื่อแลกกับการปลดล็อกข้อมูลเหล่านั้น

"ดูแลบัญชีของบริษัทเสมือนกับเป็นข้อมูลส่วนตัวของคุณเอง"

DO	DON'T
ใช้บัญชีระบบของบริษัท/อีเมลของบริษัทกับ ***อุปกรณ์ที่ได้รับอนุญาตเท่านั้น** *(เช่น อุปกรณ์ของบริษัท หรืออุปกรณ์ที่ลงทะเบียนไว้กับบริษัทแล้ว)*	ไม่ใช้บัญชีระบบของบริษัท/อีเมลของบริษัทกับ ***อุปกรณ์ที่ไม่ได้รับการอนุญาต** *(เช่น อุปกรณ์ส่วนตัวที่ไม่ได้ลงทะเบียนไว้กับบริษัท)*

Source: Toyota Asia Cybersecurity Team