


Cybersecurity Bulletin

Credential Leak: A Close and Dangerous Threat!

Protect your digital life: understanding credential leaks is the first step. Learn how easily your usernames and passwords can fall into the wrong hands and what you can do to prevent it.

Credential

are Username, Password and Other Sensitive information such as Security questions, PINs, and other personal data used for verification.



Credential Leak

A credential leak occurs when these sensitive pieces of information are exposed or compromised, making them available to unauthorized individuals. This exposure can happen in various ways and leads to severe security risks.



How Credentials Are Leaked:




Data Breaches

Large-scale data leaks that expose millions of credentials.



Malware

Malicious software that can steal credentials from infected devices.



Phishing Attacks


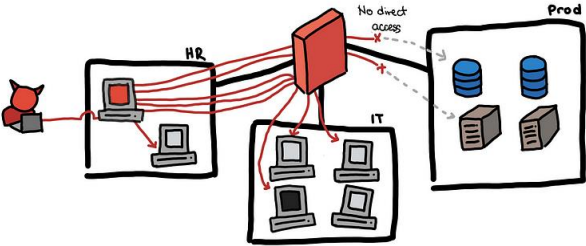


Deceptive emails or messages designed to trick users into revealing their credentials.

Cybersecurity Bulletin

Credential Leak: A Close and Dangerous Threat!

What Attackers Do with Stolen Credentials

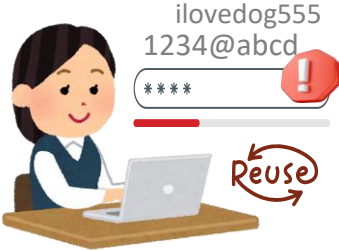


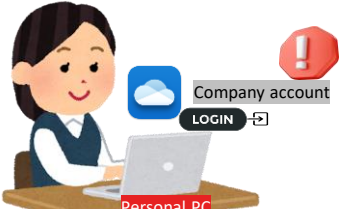











Attackers leverage stolen credentials in a variety of ways, including:

	<p>Account Takeover (ATO) & Identity Theft</p> <p>Attackers use your credentials to gain access to your online accounts, such as email, social media, or banking. With access to your accounts, attackers can steal your identity and use it to open new accounts, apply for loans, or commit fraud.</p>
	<p>Lateral Movement</p> <p>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.</p>
	<p>Ransomware Attacks</p> <p>Attackers may use stolen credentials to gain access to critical systems and deploy ransomware, encrypting data and demanding payment for its release.</p>
	<p>Espionage</p> <p>Attackers can use stolen credentials to access confidential information, such as trade secrets or customer data, for competitive advantage or to sell on the dark web.</p>

Cybersecurity Bulletin

Credential Leak: A Close and Dangerous Threat!

Common risky behaviors that can lead to credential leaks.

	<div>DON'T</div> <div></div> <div>Poor password hygiene<ul style="list-style-type: none">Using Weak or Reused Passwords.Sharing passwords with others, even within organizations.</div>
	<div>DO</div> <div></div> <div>Use Strong, Unique Passwords / Keep Your Credentials Private<ul style="list-style-type: none">Create complex passwords with a mix of uppercase, lowercase, numbers, and special characters. Use a password manager to store them securely.Never share your passwords or authentication details with anyone. Use multi-factor authentication (MFA) for added security.</div>
	<div>DON'T</div> <div></div> <div>Use corporate account log-in to personal devices<p>Personal devices may not have adequate security, increasing the risk of compromise or unauthorized access due to limited advanced detection.</p></div>
	<div>DO</div> <div></div> <div>Use Only Approved Company Devices<p>Always use company-authorized devices for work to ensure security compliance and data protection.</p></div>
	<div>DON'T</div> <div></div> <div>Use/Download crack or illegal software<p>Do not download and install any software on company device without authorization given.</p></div>
	<div>DO</div> <div></div> <div>Use company permitted software / legitimate software<p>In case of new software installation is required. Please request through IT Service Systems or contact IT helpdesk.</p></div>
	<div>DON'T</div> <div></div> <div>Falling for Phishing Attacks<p>Clicking on malicious links or downloading attachments can lead to credential theft.</p></div>
	<div>DO</div> <div></div> <div>Verify Before Clicking<p>Always check the sender and URL before clicking links or downloading files. Report suspicious emails to IT security.</p></div>
	<div>DON'T</div> <div></div> <div>Using Public Wi-Fi Without Caution<p>Connecting to unsecured Wi-Fi networks can expose your credentials to hackers.</p></div>
	<div>DO</div> <div></div> <div>Use Secure Connections<p>Avoid public Wi-Fi for sensitive work. Use a VPN when necessary to encrypt your internet traffic.</p></div>

By understanding the risks and taking proactive measures, we can significantly reduce the likelihood of credential leaks and protect our company and ourselves.

Cybersecurity Bulletin

การรั่วไหลของข้อมูลประจำตัว: ภัยคุกคามที่ใกล้ตัวและอันตราย!

ปกป้องชีวิตดิจิทัลของคุณ: การเข้าใจการรั่วไหลของข้อมูลประจำตัวคือขั้นตอนแรก
เรียนรู้วิธีที่ผู้ใช้และรหัสผ่านของคุณสามารถตกไปอยู่ในมือของผู้ไม่หวังดีได้อย่างง่ายดาย
และสิ่งที่คุณสามารถทำได้เพื่อป้องกัน

Credential
(ข้อมูลประจำตัว)

คือ ชื่อผู้ใช้ รหัสผ่าน และข้อมูลสำคัญอื่นๆ เช่น
คำถามรักษาความปลอดภัย รหัส PIN และข้อมูล
ส่วนตัวอื่นๆ ที่ใช้สำหรับการยืนยันตัวตน

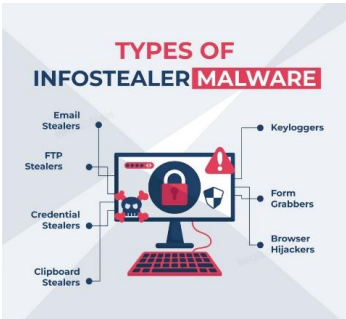


Credential Leak
(การรั่วไหลของข้อมูลประจำตัว)

เกิดขึ้นเมื่อข้อมูลสำคัญเหล่านี้ถูกเปิดเผยหรือถูก
โจรกรรม ทำให้บุคคลที่ไม่ได้รับอนุญาตสามารถเข้าถึง
ได้ การเปิดเผยนี้สามารถเกิดขึ้นได้หลายวิธีและนำไปสู่
ความเสี่ยงด้านความปลอดภัยที่ร้ายแรง



ข้อมูลประจำตัวรั่วไหลได้อย่างไร:



การละเมิดข้อมูล

การรั่วไหลของข้อมูลขนาดใหญ่ที่
เปิดเผยข้อมูลประจำตัวนับล้าน

มัลแวร์

ซอฟต์แวร์ที่เป็นอันตรายที่สามารถ
ขโมยข้อมูลประจำตัวจากอุปกรณ์ที่
ติดไวรัส

การโจมตีแบบฟิชชิง

อีเมลหรือข้อความหลอกลวงที่
ออกแบบมาเพื่อหลอกให้ผู้ใช้
เปิดเผยข้อมูลประจำตัวของตน

Cybersecurity Bulletin

การรั่วไหลของข้อมูลประจำตัว: ภัยคุกคามที่ใกล้ตัวและอันตราย!

ผู้โจมตีทำอะไรกับข้อมูลประจำตัวที่ถูกขโมย

ผู้โจมตีใช้ประโยชน์จากข้อมูลประจำตัวที่ถูกขโมยด้วยวิธีการต่างๆ ซึ่งรวมถึง:

	<p>Account Takeover (ATO) & Identity Theft (การยึดบัญชี และการโจรกรรมข้อมูลส่วนบุคคล)</p> <p>ผู้โจมตีใช้ข้อมูลประจำตัวของคุณเพื่อเข้าถึงบัญชีออนไลน์ของคุณ เช่น อีเมล โซเชียลมีเดีย หรือบัญชีธนาคาร เมื่อเข้าถึงบัญชีของคุณได้แล้ว ผู้โจมตีสามารถขโมยข้อมูลส่วนบุคคลของคุณและนำไปใช้เปิดบัญชีใหม่ สมัครสินเชื่อ หรือก่ออาชญากรรม</p>
	<p>Lateral Movement (การเคลื่อนที่ในแนวนอน)</p> <p>ในสภาพแวดล้อมขององค์กร ผู้โจมตีใช้ข้อมูลประจำตัวของพนักงานที่ถูกโจรกรรมเพื่อเคลื่อนที่ไปตามเครือข่าย เข้าถึงระบบและข้อมูลที่สำคัญยิ่งขึ้น ซึ่งอาจนำไปสู่การละเมิดข้อมูลครั้งใหญ่ การโจรกรรมทรัพย์สินทางปัญญา หรือการหยุดชะงักของการดำเนินงาน</p>
	<p>Ransomware Attacks (การโจมตีด้วยแรนซัมแวร์)</p> <p>ผู้โจมตีอาจใช้ข้อมูลประจำตัวที่ถูกขโมยเพื่อเข้าถึงระบบที่สำคัญและติดตั้งแรนซัมแวร์ เข้ารหัสข้อมูล และเรียกค่าไถ่เพื่อแลกกับการปลดล็อกข้อมูล</p>
	<p>Espionage (การจารกรรม)</p> <p>ผู้โจมตีสามารถใช้ข้อมูลประจำตัวที่ถูกขโมยเพื่อเข้าถึงข้อมูลที่เป็นความลับ เช่น ความลับทางการค้าหรือข้อมูลลูกค้า เพื่อความได้เปรียบทางการแข่งขัน หรือเพื่อขายในตลาดมืด</p>

Cybersecurity Bulletin

การรั่วไหลของข้อมูลประจำตัว: ภัยคุกคามที่ใกล้ตัวและอันตราย!

พฤติกรรมเสี่ยงที่อาจนำไปสู่การรั่วไหลของข้อมูลประจำตัว

	DON'T 	สวชนนณมยรห้สผนท่ไม่ด้ <ul style="list-style-type: none">การใชรห้สผนท่ไม่พลอดกยหรือนารห้สผนท่เคยใช้แล้วมาใชซ้ำการแบ่งปันรห้สผนกับผู้อื่น แม้แต่ภายในองค์กร
	DO 	ใชรห้สผนท่แข็งแกรงและไม่ซ้ำกัน / เก็บข้อมูลประจำตัวของคุณเป็นส่วนตัว <ul style="list-style-type: none">สร้างรห้สผนท่ซับซ้อนโดยใชตัวพิมพ์ใหญ่ ตัวพิมพ์เล็ก ตัวเลข และอักขระพิเศษ ผสมกัน ใชโปรแกรมจัดการรห้สผนเพื่จัดเก็บอย่างพลอดกยห้ามแบ่งปันรห้สผนหรือรายละเอียดการยืนยันตัวตนของคุณกับใครก็ตาม ใชการยืนยันตัวตนแบบหลายปัจจัย (MFA) เพื่เพิ่มความพลอดกย
	DON'T 	ใชบัญชีบริษัทล็อกอินเข้าอุปกรณ์ส่วนตัว <ul style="list-style-type: none">อุปกรณ์ส่วนตัวอาจไม่มีระบบรักษาความปลอดภัยที่เพียงพอ ทำให้ความเสี่ยงต่อการถูกโจรกรรมหรือการเข้าถึงโดยไม่ได้รับอนุญาตเพิ่มขึ้น เนื่องจากข้อจำกัดในการตรวจจับชั้นสูง
	DO 	ใชอุปกรณ์ที่บริษัทอนุมัติเท่านั้น <ul style="list-style-type: none">ใชอุปกรณ์ที่บริษัทอนุมัติสำหรับงานเสมอ เพื่ให้มั่นใจถึงการปฏิบัติตามข้อกำหนดด้านความปลอดภัยและการปกป้องข้อมูล
	DON'T 	ใช/ดาวน์โหลดโปรแกรมแคร็กหรือโปรแกรมผิดกฎหมาย <ul style="list-style-type: none">ห้ามดาวน์โหลดและติดตั้งซอฟต์แวร์ใดๆ บนอุปกรณ์ของบริษัทโดยไม่ได้รับการอนุมัติ
	DO 	ใชซอฟต์แวร์ที่บริษัทอนุญาต / ซอฟต์แวร์ที่มีลิขสิทธิ์ถูกต้อง <ul style="list-style-type: none">ในกรณีนี้จำเป็นต้องติดตั้งซอฟต์แวร์ใหม่ โปรดดำเนินการผ่านระบบ IT Service Systems หรือติดต่อ IT helpdesk
	DON'T 	ตกเป็นเหยื่อของการโจมตีแบบฟิชซิง <ul style="list-style-type: none">การคลิกลิงก์ที่เป็นอันตรายหรือการดาวน์โหลดไฟล์แนบอาจนำไปสู่การโจรกรรมข้อมูลประจำตัว
	DO 	ตรวจสอบก่อนคลิก <ul style="list-style-type: none">ตรวจสอบผู้ส่งและ URL เสมอก่อนคลิกลิงก์หรือดาวน์โหลดไฟล์ รายงานอีเมลที่น่าสงสัยไปยังฝ่ายรักษาความปลอดภัย IT
	DON'T 	ใช Wi-Fi สาธารณะโดยไม่ระมัดระวัง <ul style="list-style-type: none">การเชื่อมตอกับเครือข่าย Wi-Fi ท่ไม่พลอดกยอาจทำให้ข้อมูลประจำตัวของคุณเสี่ยงต่อการถูกแฮกเกอร์โจรกรรม
	DO 	ใชการเชื่อมต่อที่พลอดกย <ul style="list-style-type: none">หลีกเลี่ยงการใช้ Wi-Fi สาธารณะ เชื่อมต่อ VPN เพื่เข้ารหัสการรับส่งข้อมูลทางอินเทอร์เน็ตของคุณ

การทำความเข้าใจถึงความเสี่ยงและการดำเนินการมาตรการเชิงรุก สามารถลดโอกาสการรั่วไหลของข้อมูลประจำตัวได้อย่างมาก ปกป้องทั้งบริษัทและตัวเราเอง