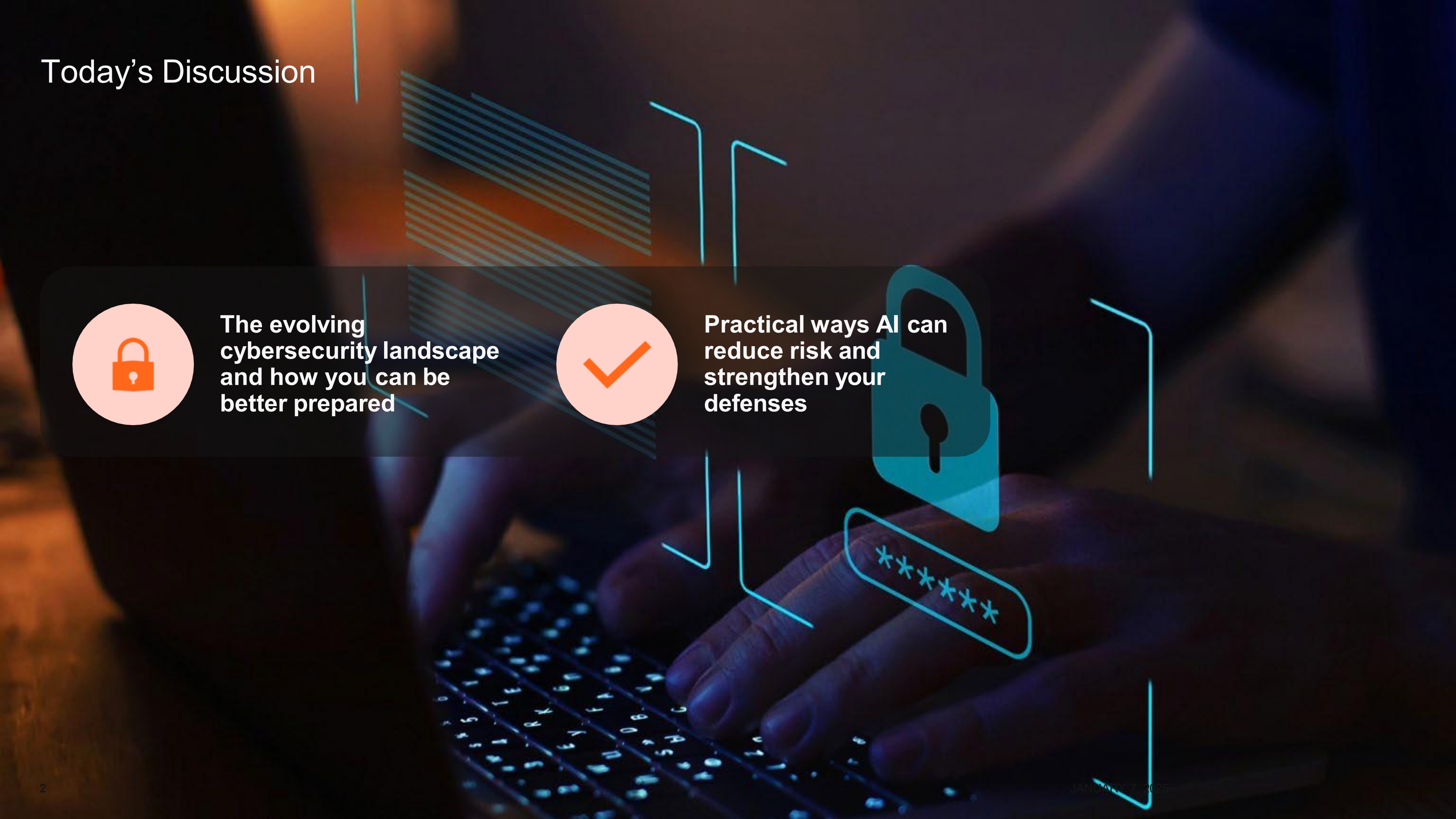
Practical AI and Cybersecurity

Brought to you by Mastercard Digital Doors®

Today’s Discussion



- The evolving cybersecurity landscape and how you can be better prepared
- Practical ways AI can reduce risk and strengthen your defenses

No individual, business, or organization is safe from cyberattacks

Employees of small businesses experience **350%** more social engineering attacks than those at larger enterprises. [1]

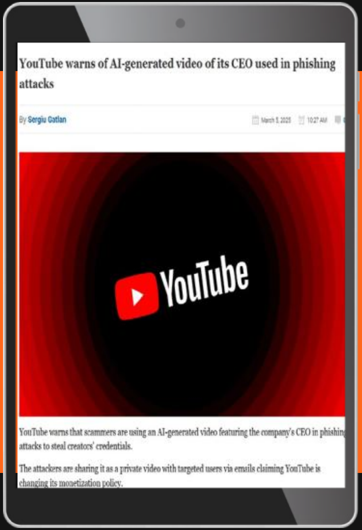
There was a **20%** increase in data breaches from 2022 to 2023.[2]

75% of SMBs could not continue operating if they were hit with ransomware. [3]

51% of cyberattacks are powered by Artificial Intelligence (AI) [4]

1. Report: Small businesses receive 350% more social engineering attacks than enterprises, mostly from Microsoft impersonators - ITOps
2. TimesThe-Continued-Threat-to-Personal-Data-Key-Factors-Behind-the-2023-Increase.pdf (apple.com)
3. Why small businesses are at greater risk of malware attacks | LinkedIn
4. Cyber Attacks are More Sophicated Than Ever, With AI-Powered Attacks Posting hte Greatest Risk (March 26, 2024)

The headlines can be scary!



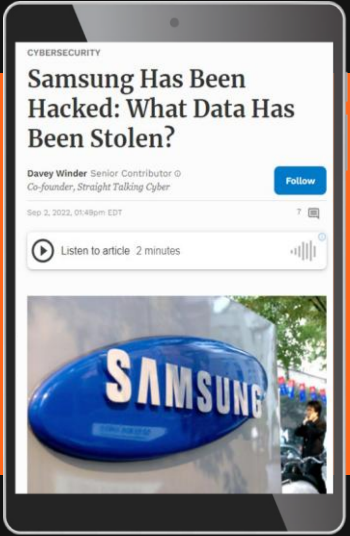
YouTube warns of AI-generated video of its CEO used in phishing attacks

By Sergiu Gatlan March 5, 2025 10:27 AM

YouTube warns that scammers are using an AI-generated video featuring the company's CEO in phishing attacks to steal creators' credentials.

The attackers are sharing it as a private video with targeted users via emails claiming YouTube is changing its monetization policy.

93% of companies anticipate they will face daily AI-powered cyber attacks in the next 6 months[1]



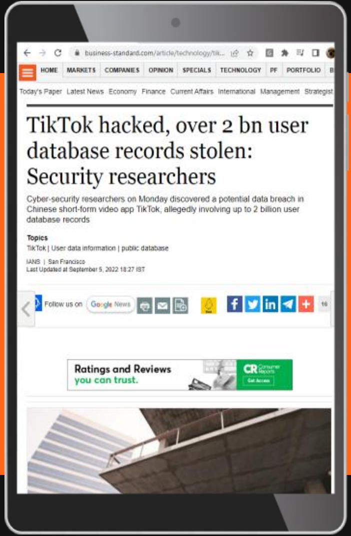
CYBERSECURITY

Samsung Has Been Hacked: What Data Has Been Stolen?

Davey Winder Senior Contributor
Co-founder, Straight Talking Cyber

Sep 2, 2022, 01:49pm EDT

91% of companies will experience a phishing attack[2]



business-standard.com/article/technology/tik...

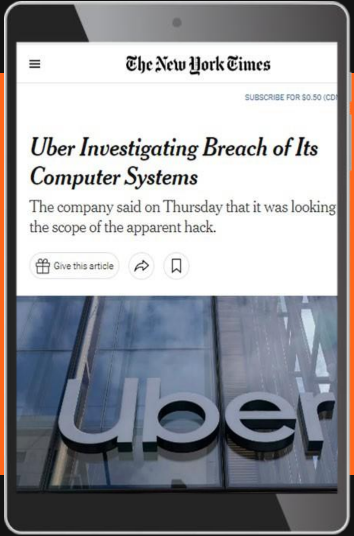
TikTok hacked, over 2 bn user database records stolen: Security researchers

Cyber-security researchers on Monday discovered a potential data breach in Chinese short-form video app TikTok, allegedly involving up to 2 billion user database records

Topics
TikTok | User data information | public database

IANS | San Francisco
Last Updated at September 5, 2022 18:27 IST

27% of companies will be hit by ransomware[2]



The New York Times

SUBSCRIBE FOR $0.50 (CD

Uber Investigating Breach of Its Computer Systems

The company said on Thursday that it was looking the scope of the apparent hack.

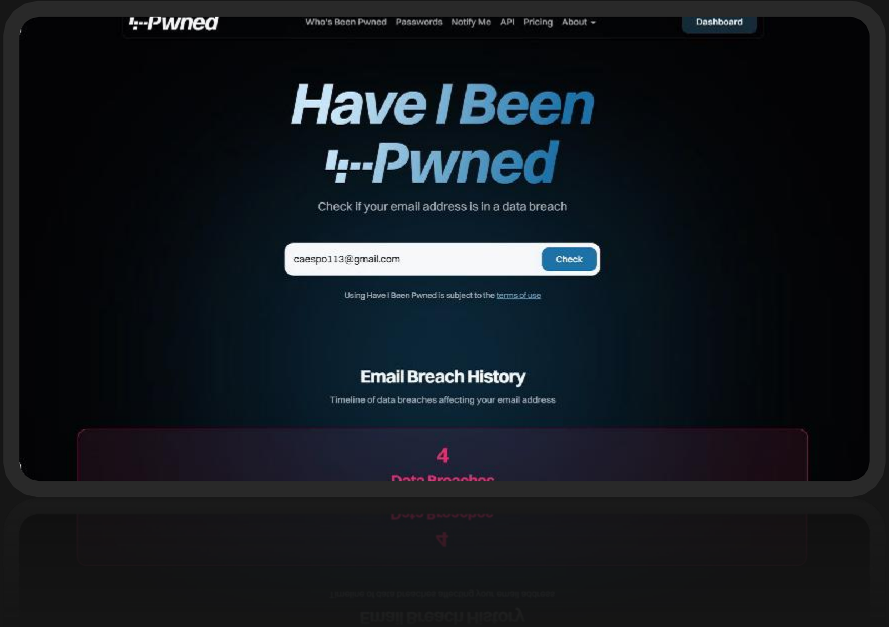
27% of companies will be affected by a business email compromise[2]

Don’t be fooled into thinking you are immune to cyberattacks just because you don’t see reports of attacks on small businesses in the news!

1. https://purplesec.us/ AI-Powered Cyber Attacks: The Future Of Cybercrime, June 10, 2025
2. Aite (2023), Threat research is based 30 independent threat reports curated and analyzed

Ways you can protect your business

Implement Strong Password Policies



Have I Been Pwned

Check if your email address is in a data breach

caespo113@gmail.com

Using Have I Been Pwned is subject to the terms of use

Email Breach History

Timeline of data breaches affecting your email address

4

Data Breaches

In 80% of all hacking cases, compromised credentials or passwords are to blame

Preventative Measures

- Require complex, unique passwords or passphrases for all employees
- Encourage the use of password managers or password generators
- Enforce regular password changes and discourage reuse

Tools that can help

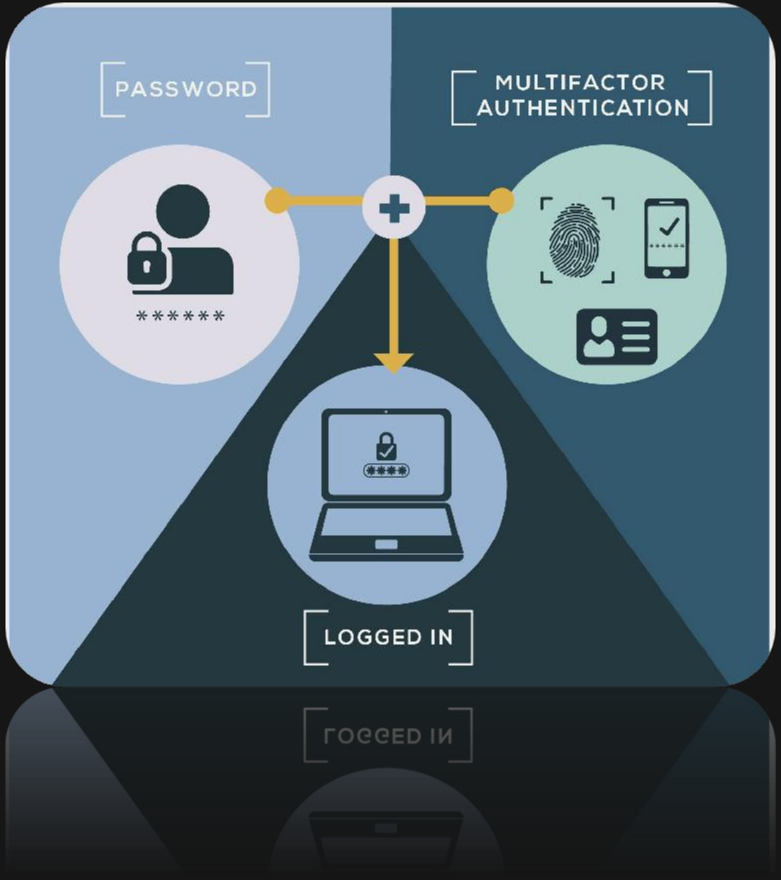
- Password Manager
- Google Workspace
- Microsoft 365

LastPass •••|

1Password

Source: Astra Security Jan 9, 2025

Multi-Factor Authentication (MFA)



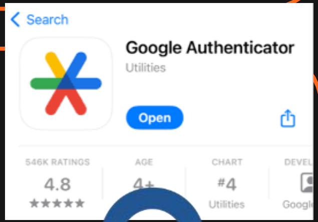
Passwords alone are not enough due to rising credential stuffing and brute force attacks

Preventative Measures

- Enforce MFA for all critical accounts
  - Email
  - Financial systems
  - Cloud services

Tools that can help

- Google Authenticator
- Microsoft Authenticator



Ransomware Protection & Response

Over 22% of all cyber attacks on small businesses were Ransomware

Preventative Measures

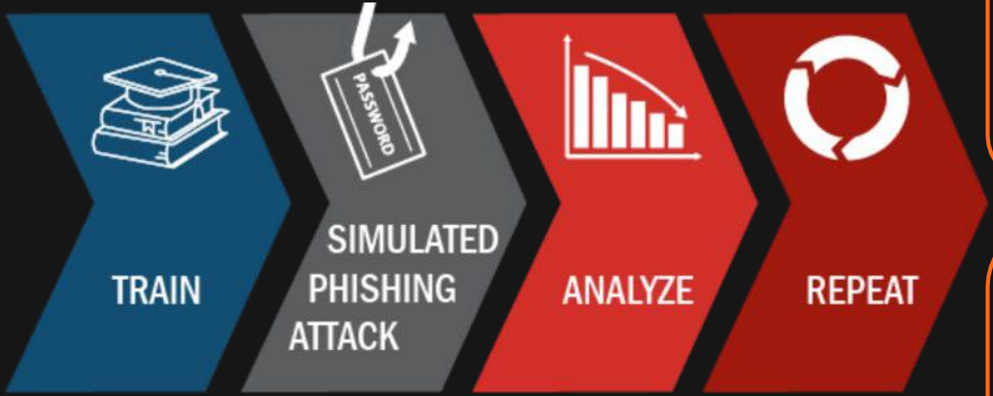
- Regular backups and disaster recovery strategies
- Employee training on phishing and social engineering
- Multi-layered defense systems
- Create an Incident Response Plan

Tools that can help

- Anti-ransomware software
- www.NoMoreRansom.org
- Cyber Insurance

Source: Mastercard Cyber Insights Data
Based on data for Jan 1 – Dec 31, 2024

Employee Training and Awareness



95% of all cyber attacks are caused by human error

Preventative Measures

- Regular cybersecurity training programs which include AI awareness
- Teach employees how to identify phishing attempts, manage passwords securely, and follow data protection practices

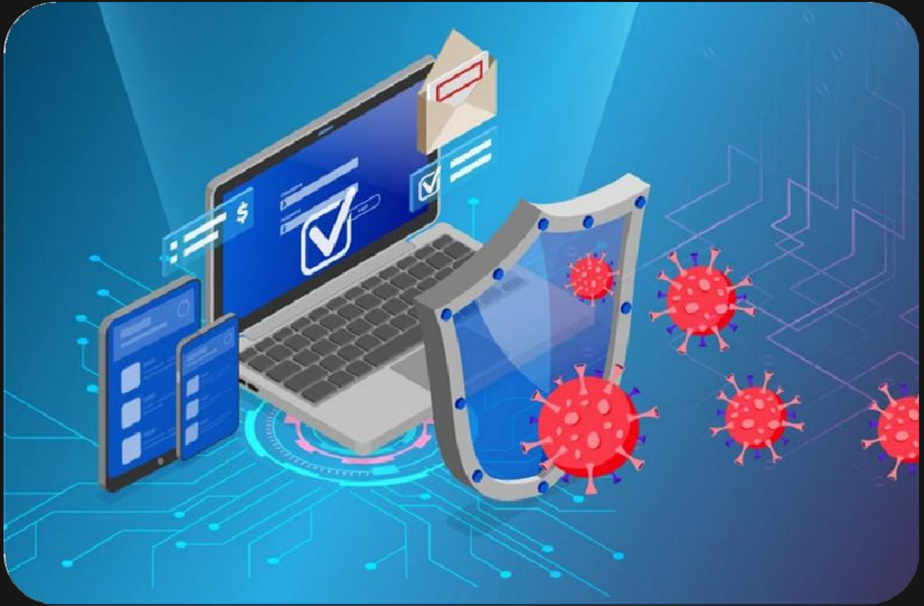
Tools that can help

- Phishing simulations, HacWare
- Training and Education platforms, Mastercard Trust Center, Cybersecurity Assessment Quiz, Small Business Navigator
- Cyber Readiness Institute
- GCA Cybersecurity Toolkit for Small Business

Source: World Economic Forum

Endpoint Protection

Remote work has expanded the number of vulnerable devices accessing corporate networks



Preventative Measures

- Deploy Endpoint Detection and Response (EDR) tools
- Ensure regular patching and updates for all software and systems

Tools that can help

- Antivirus software McAfee Norton
- Virtual Private Network (VPN)
- Separate employee & guest networks
- Malware solutions Malwarebytes

Artificial Intelligence and Automation for Threat Detection

AI can speed up threat detection and automate response to mitigate breaches quickly

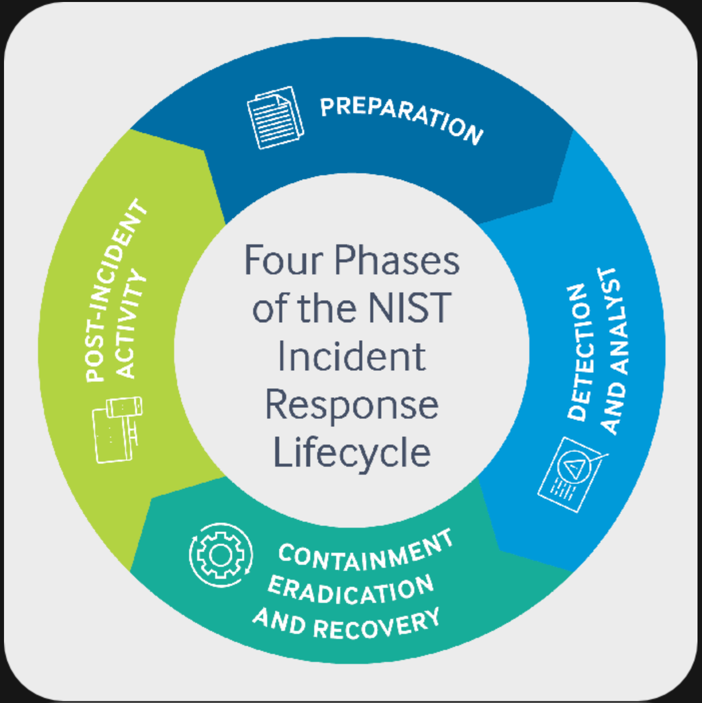
Preventative Measures

- Integrate AI-powered threat detection tools into your security strategy
- Create an AI Acceptable Use-Policy (AUPs)

Tools that can help

- AI-driven SIEM (Security Information and Event Management)
- Automated threat detection
- Security orchestration platforms
- Privacy settings

Incident Response and Recovery Planning


PREPARATION
DETECTION AND ANALYST
CONTAINMENT ERADICATION AND RECOVERY
POST-INCIDENT ACTIVITY
Four Phases of the NIST Incident Response Lifecycle

$25K small businesses typically lose due to cyber attacks

Preventative Measures

- Develop and regularly update incident response plans
- Create business continuity plans for rapid recovery after a breach

Tools that can help

- Forensic tools
- Back up solutions
- Incident response plan

Source: Astra Security Jan 9, 2025
NIST- National Institute of Standards and Technology

AI Tools & Directory

- ChatGPT: Generates text responses to questions and prompts.
- Perplexity: Provides answers based on web research.
- ElevenLabs: Creates synthetic voices for audio content.
- HeyGen: Produces video content using AI avatars.
- Runway ML: Edits images and videos using AI tools.
- Midjourney: Generates images from text descriptions.
- Udio: Manages scheduling and appointments.
- Zapier: Connects apps to automate workflows.
- Make: Builds automated workflows between apps.
- Airtable: Organizes data in a flexible spreadsheet-database format.
- HacWare: An AI-powered platform that automates security awareness training and phishing simulations to help businesses reduce human risk.

Protect your Online Business like you would your Own Home

> “It takes 20 years to build a reputation and a few minutes of a cyber-incident to ruin it.”

Stephane Nappo

Global Head Info Security,
Societe General International Banking

Thank you

Tiffany Ricks

CEO, HacWare
hello@hacware.com

Carolyn Esposito

Director, Security Solutions
Carolyn.esposito@mastercard.com