Devising a modern MFA-strategy in an AI world

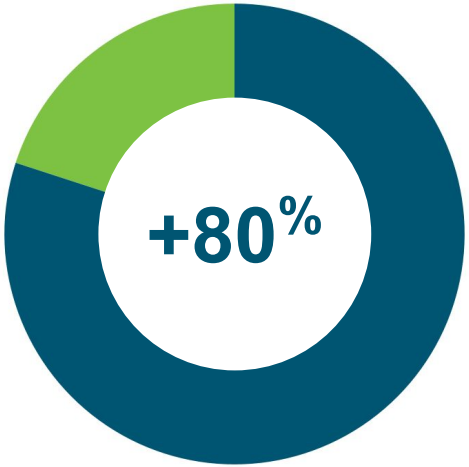
17 October 2024

Fredrik Hallberg
Sales Director - Key Accounts Nordics & Baltics
Yubico

Overview

- The rise of AI in cyber fraud
- The risks of cyber fraud
- The role of authentication
- Key takeaways

The rise of generative AI in cyber security



Cyber attacks start with phishing and will grow with AI-driven phishing attacks[1]

US FTC's Khan says Agency already seeing AI used to 'turbocharge' fraud, scams[2]

1. Comcast. Business Cybersecurity Threat Report. 2023
2. Bloomberg. FTC's Khan Says Enforcers Need to Be 'Vigilant Early' With AI. 2023

Today attackers don't hack in, they login

Apr 12, 13:00 27°C 68%

The Standard 英文虎報

Access. Untethered.
Mobile workflows for BYOD
and shared-use environment.

Trending | Section News | Features | Event & Promotion | Coffee Break

Top News Editorial Local Finance China World Sports Central Station Columns

Human error suspected in Cyberport data leak

Local | 13 Sep 2023 11:38 am

A Cyberport Board Director said on Wednesday that huma
with the investigation set to look into whether the 400 giga
information was stored on a shared drive in their system.

The personal data of staff from Cyberport and some startu
numbers, bank statements and resumes - were released c
flagship's servers were hacked last month.

Latitude Financial warns customer data breach could widen and hack 'remains active'

By business reporter Emilia Terzon

Posted Mon 20 Mar 2023 at 1:05pm, updated Fri 24 Mar 2023 at 9:54am

maurice blackburn lawyers

Injury & illness Class

Home › Class actions › Join a class action › Medibank Data Breach

Medibank Data Breach Investigation and Complaint

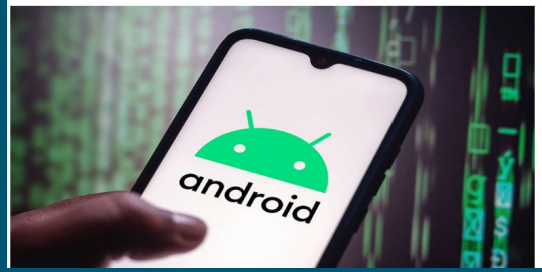
Maurice Blackburn has made a representative complaint to the Office of the Australian Information Commissioner (OAIC) against Medibank

Crime, Singapore

Singapore Police issues alert over malware scams as two victims lose nearly S$100k in CPF savings

Singapore Police caution Android users after two victims lose nearly S$100k from their CPF savings to a new strain of phishing malware scams.

14 comments



POPULAR POSTS

Singaporean ex-S-League coach in China prison suffered heart attack and coma last week

MP slams hooded student at NYP graduation ceremony

23,100 new citizenships granted in 2022 but only 3,400 new citizens serve NS each year

No warning issued to influencer Xiaxue for offensive online comments, but WP's MP

The business of faking it

Phish-as-a-service toolkits are getting better. User vigilance is not enough

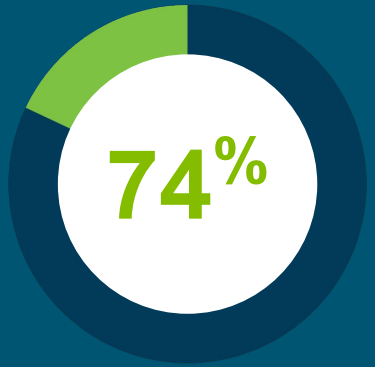
Campaigns only need to be fractionally better for huge gains. Some reports show spear phishing click rates at over 50%[1].

[1] StationX, Top Phishing Statistics for 2024: Latest Figures and Trends, 2023

Growing number of phishing toolkits available. The bar to entry for phishing is lower than ever[2].

[2] Quick, cheap and dangerous: how scammers are creating thousands of fake pages using phishing kits

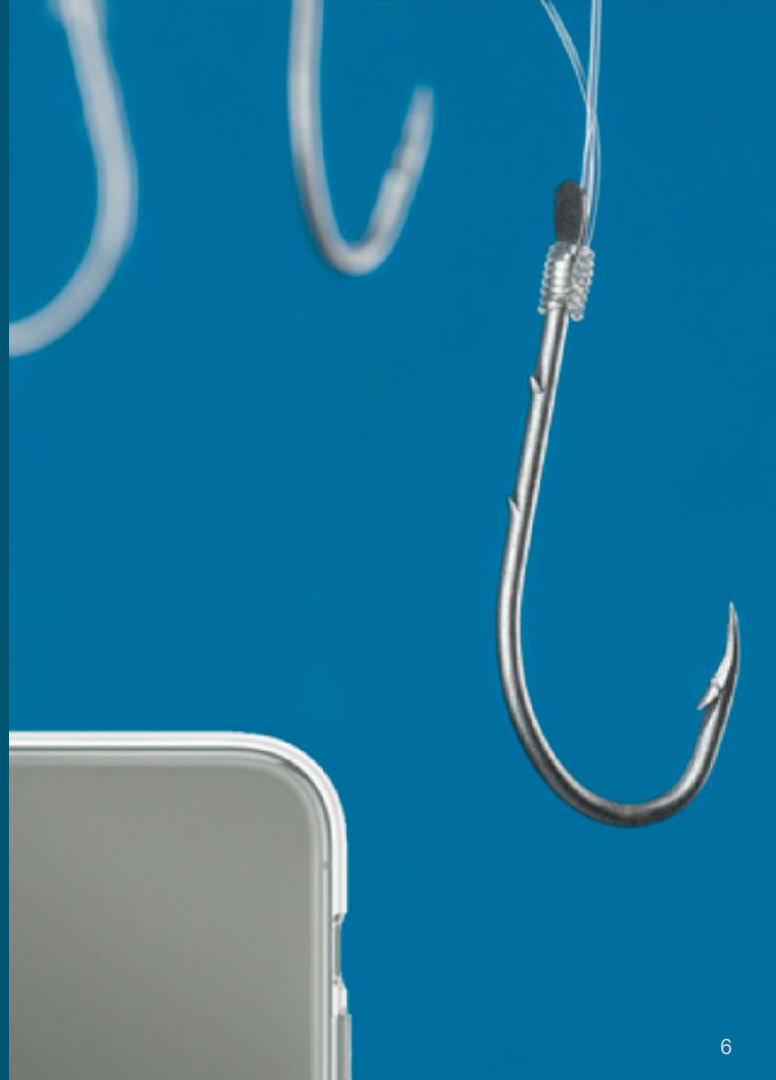
The human element is the target!



Verizon DBIR 2023 ..81% of hacking related breaches caused by weak or stolen passwords of which 74% were influenced by human-related factors[1]

200-300%

increase in cyber insurance rates[2]



1. Verizon DBIR 2023
2. Business Insurance, Hospitality sector steps up risk controls as cyber, other threats rise, February 2022

Strong authentication to safeguard credentials

Any form of MFA is better than none, but . . .

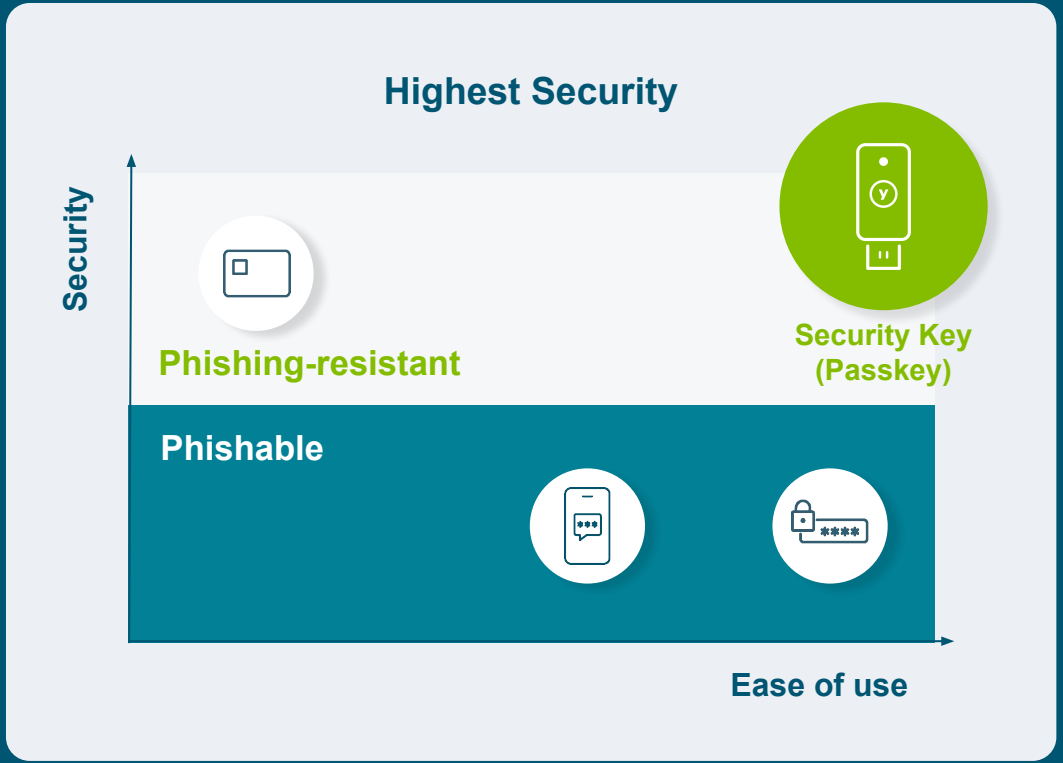
Not all MFA is created equal

- Convenient forms of MFA can be phished

Ease of use encourages adoption

Remove reliance on user vigilance

- AI is convincing



Human elements - secure by design

Since 2014

1960s

Usernames and passwords

Login

2014

FIDO U2F Phishing-resistant second factor

yubico Google

2019

FIDO2/WebAuthn Phishing-resistant

Second factor

Multi-factor/ Passwordless

2022

PassKeys

Multi-factor/Passwordless (device bound or syncable)

Google Microsoft

Mitigation - Reactive or proactive?

Reactive Response (Assume Breach)

- More Training
- Cyber insurance
- Convenient MFA
- Greater fines

Proactive Response

- Adopt Zero Trust
- Leverage tech that removes reliance on vigilance of the user
- Deploy phishing resistant MFA

What exactly is phishing-resistant MFA?

Based on trust relationship

Registration process needs to be protected

No shared secrets

Which could be easily stolen

Possession based

Private keys are securely stored in something I have

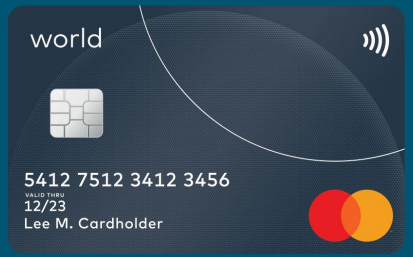
Know the transacting parties

Both user and relying party are aware of each other

User Intent

User acts on a known initiated authentication request

Familiar human elements facilitate adoption



Present
Vigilance
Trust

Knowledge
Familiarity
Simplicity

Biometric
Touch
User Intent

Without reliance on the vigilance of the user*

*NIST SP800-63B

Key takeaways

1

AI and the usage of tools will be an accelerator for phishing campaigns.

2

No amount of user training can keep pace with the rate of sophistication available to attackers.

3

Organizations need to focus on what is effective: phishing-resistant systems & users.

Thank you!

Questions / Comments

Email: fredrik.hallberg@yubico.com

yubico