Cyber Threat Landscape

Shifting Sands – Trends in Cybersecurity

Abbas Kudrati

APAC Chief Cybersecurity Advisor
Microsoft

Industry Professor
Deakin University

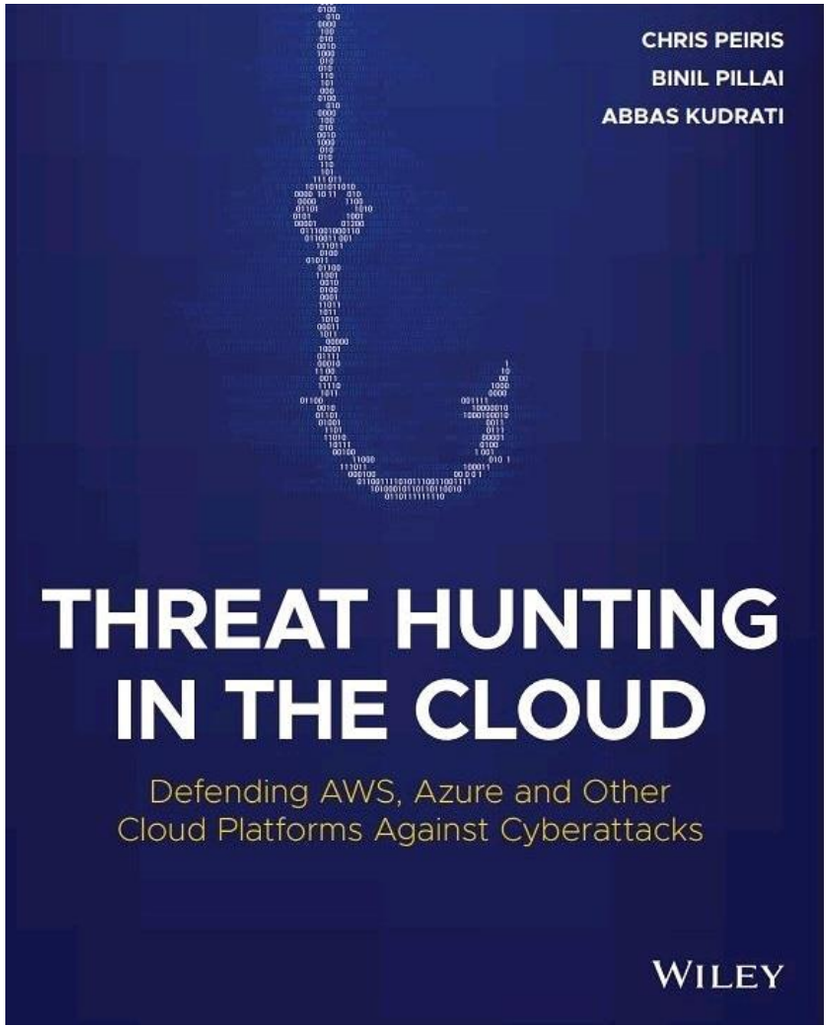
Microsoft

About me

"You join Microsoft, not to be cool
but to make others cool"
Satya Nadella

- **Cybersecurity practitioner and CISO with 25+ years of experience in Information / Cybersecurity.**
- **Part time Cybersecurity Professor with Deakin and LaTrobe University in Melbourne, Australia.**
- **Expertise in Zero Trust, Cybersecurity Strategy, Security Operations, Risk, Compliance, Cloud Security and Architecture.**

Upcoming books



Releasing in Sept 2021, Pre-order on Amazon.

Work in progress

Zero Trust Journey across the Digital Estate

By

Abbas Kudrati & Binil Pillai

CRC Press
Taylor & Francis Group

Target release by Feb 2022.

Work in progress

Digitization Risks in Post Pandemic World

By

Ashish Kumar, Abbas Kudrati & Shashank Kumar

Packt

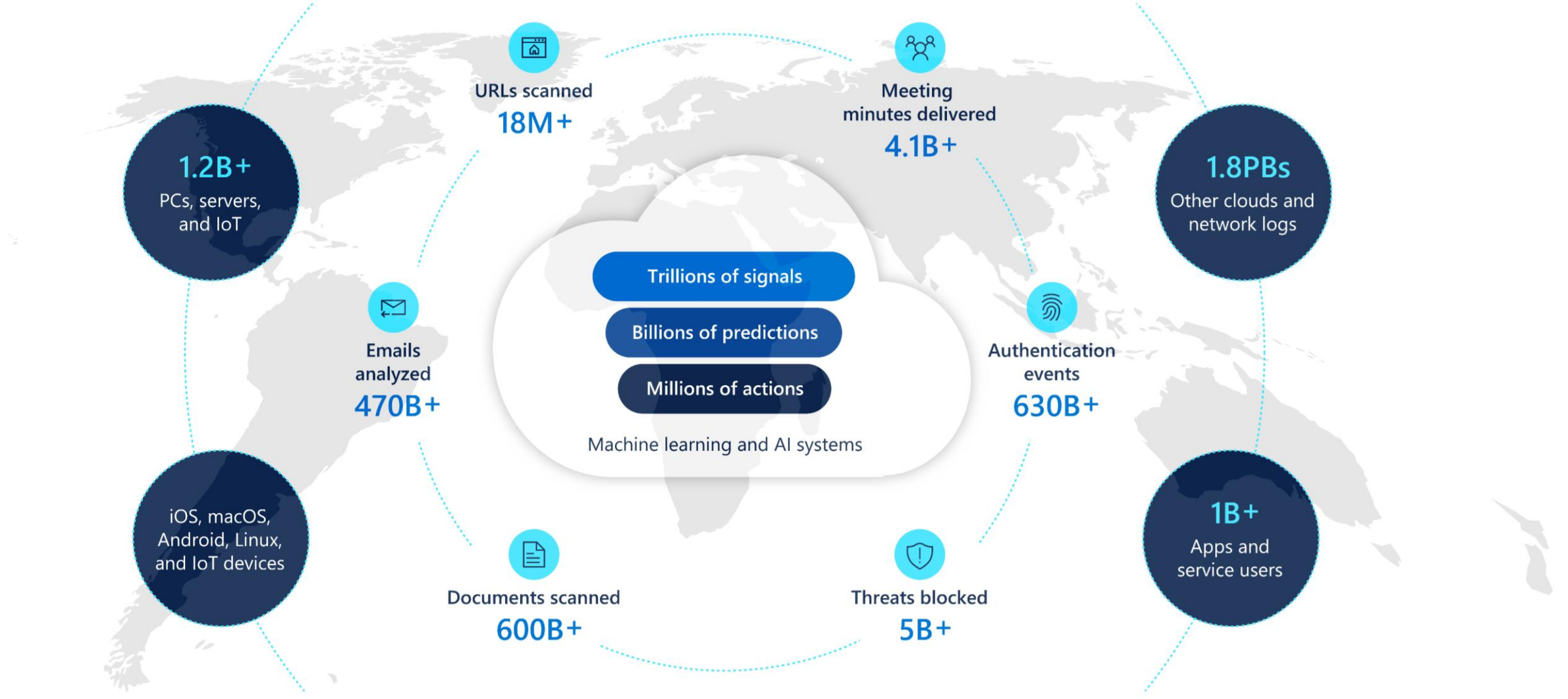
Target release by March 2022.

Topics

- Australia’s Cyber Threat Landscape
- Password Security
- Live Demos and Examples – How Hackers Hack !
- Recommendations
- Q & A

Unique insights informed by trillions of signals

Monthly volume and diversity of signals used by Microsoft security operations



Australia’s Cyber Threat Landscape

MALWARE

Code developed by cyber attackers, designed to cause extensive damage to data and systems or to gain unauthorized access to a network

Malware encounter rate across Asia Pacific

5.34%

(↓23% from 2018)

1.6 times higher than the global average

Countries with highest encounter rate

1. Indonesia
2. Sri Lanka
3. Vietnam

Countries with lowest encounter rate

1. Japan
2. New Zealand
3. Australia

Malware trends in Asia Pacific

Cybercriminals remain focused on attacking countries with:

- Lower levels of cyber awareness
- High usage of unlicensed and/or pirated software, and sites that illegitimately offer free software or content

Microsoft

3rd

Lowest encounter rate in Asia Pacific

Ranked #14 in 2018

MALWARE

Australia's malware encounter rate was 4.3 times lower than the regional and 2.6 times lower than the global average.

Highest Encounter Rate

1. Indonesia
2. Sri Lanka
3. Vietnam

Lowest Encounter Rate

1. Japan
2. New Zealand
3. Australia

Source: security endpoint threat report 2019

Microsoft

RANSOMWARE

Malicious software that disables a device or its files until the attacker is paid a ransom

Ransomware encounter rate across Asia Pacific

0.05%

(↓29% from 2018)

1.7 times higher than the global average

Countries with highest encounter rate

1. Vietnam
2. Indonesia
3. India

Countries with lowest encounter rate

1. Japan
2. New Zealand
3. Australia

Ransomware trends in Asia Pacific

Even with a slowdown in ransomware encounters, cyber attackers are shifting their efforts to customized campaigns targeting specific:

- Geographical areas
- Industries
- Businesses

Microsoft

3rd

Lowest encounter rate in Asia Pacific

Ranked #14 in 2018

RANSOMWARE

Australia's ransomware encounter rate was 5 times lower than the regional and 3 times lower than the global average.

Highest Encounter Rate

1. Vietnam
2. Indonesia
3. India

Lowest Encounter Rate

1. Japan
2. New Zealand
3. Australia

Source: security endpoint threat report 2019

Microsoft

Human-Operated Ransomware Attacks

Common Attack Techniques

Initial entry through misconfigured or outdated Web servers

Credential theft and escalation of privilege

Deployment through commodity malware infection

Human-operated lateral movement

Finding and exploiting poor security controls

Disabling security controls

Human-Operated Ransomware Attacks

Defenses

Secure Internet-facing assets

Build credential hygiene

Thoroughly investigate and remediate alerts

Monitor for adversarial activities

Include IT pros in security discussions

Harden infrastructure

CRYPTOCURRENCY MINING

Malware introduced into an unsuspecting user or organization's machine(s), which then uses the machine's computing power to mine cryptocurrency

Cryptocurrency mining encounter rate across Asia Pacific

0.05%

(↓64% from 2018)

On par with the global average

Countries with highest encounter rate

1. Sri Lanka
2. India
3. Vietnam

Countries with lowest encounter rate

1. Japan
2. China
3. Australia

Cryptocurrency mining trends in Asia Pacific

Recent fluctuations in crypto-currency value and the increased time required to generate crypto-currency have resulted in attackers refocusing their efforts to target markets with:

- Low cyber awareness
- Low adoption of cyber hygiene practices

Microsoft

3rd

Lowest encounter rate in Asia Pacific

Ranked #13 in 2018

CRYPTOCURRENCY MINING

Australia's cruptocurrency encounter rate was 5 times lower than the regional and global average.

Highest Encounter Rate

1. Sri Lanka
2. India
3. Vietnam

Lowest Encounter Rate

1. Japan
2. China
3. Australia

Source: security endpoint threat report 2019

Microsoft

DRIVE-BY DOWNLOAD

Unintentional download of malicious code to a device when the user visits a website, aimed at exploiting vulnerabilities in web browsers, applications, or even the operating system

Drive-by download attack volume across Asia Pacific

0.08*

(↓27% from 2018)

On par with the global average

Countries with highest attack volume

1. Singapore
2. India
3. Hong Kong

Countries with lowest attack volume

1. New Zealand
2. Korea
3. Philippines

Drive-by download trends in Asia Pacific

Cybercriminals remain focused on stealing financial information and intellectual property.

This has resulted in key financial hubs recording the highest attack volumes in 2019.

**The Security Endpoint Threat Report records the average volume of drive-by download pages detected for every 1,000 pages indexed by Bing.*

Microsoft

12th

Highest attack volume in Asia Pacific

Ranked #6 in 2018

DRIVE-BY DOWNLOAD

Australia's drive-by-download attack volume was 2.7 times lower than the regional and global average.

Highest attack volume

1. Singapore
2. India
3. Hong Kong

Lowest attack volume

1. New Zealand
2. Korea
3. Philippines

Source: security endpoint threat report 2019

Microsoft

Recommendations from Microsoft for Staying Cybersafe

Businesses and individuals are encouraged to adopt the following best practices for cybersecurity

Guidance for businesses

- **DO:** Safeguard employees with strong tools and infrastructure
- **DO**: Turn on multi-factor authentication (MFA) as employees work from home
- **DO:** Include end-to-end encryption on trusted applications for audio/ video calling and file sharing
- **DO:** Guide employees on how to identify phishing attempts and distinguish between official communications and suspicious messages

Guidance for individuals

- **DO:** Update all devices with the latest security updates and ensure that an antivirus service is included
- **DO:** Watch out for malicious or compromised websites and avoid pirated content
- **DO**: Recognize and report suspected attack attempts
- **DO:** Verify all links and attachments before opening them

Microsoft

Password Security

Passwords are the #1 source of data theft

Credential reuse makes users even more vulnerable

Even the strongest passwords are easily phishable

81% of hacking-related breaches leveraged either stolen and/or weak passwords

OTA Cyber incidents Report 2018 I Verizon Cybercrime Case Studies 2017

An increasingly large threat landscape

230%

Increased in password spray attacks in 2020[1]

78GB

of data is uploaded monthly to risky apps by the average enterprise[1]

5B

Attacker-driven sign-ins detected in August 2020[1]

1/3

of all attacks on enterprise accounts involve phishing[1]

Type of password attack

Attack	Also Known as	Frequency	Difficulty
Credential Stuffing	Breach replay, list cleaning	Very high – 20+ million accounts probed daily	Very easy: Purchase credentials gathered from breached sites with bad data at rest policies, test for matches on other systems. List cleaning tools are readily available.
Phishing	Credential interception	Very high. 0.5% of all inbound mails.	Easy: Send emails that promise entertainment or threaten, and link user to doppelganger site for sign-in. Capture credentials. Use Modlishka or similar tools to make this very easy.
Password spray	Guessing, hammering, low-and-slow	Very high – accounts for at least 16% of attacks. Sometimes 100s of thousands broken per day. Millions	Trivial: Use easily acquired user lists, attempt the same password over a very large number of usernames. Regulate speed and distributed across many IPs to avoid detection. Tools are readily and cheaply available.

Phishing and business email compromise

Detections in the past year:

6T Messages scanned

~13B Malicious emails blocked

~1.6B URL-based email phishing threats blocked

~1.7-2B URL payloads being created each month, orchestrated through thousands of phishing campaigns

We're seeing 3 main types of phishing:

Credential phishing

Business email compromise

Combination

Top 5 spoofed brands:

Microsoft
UPS
Amazon
Apple
Zoom

Phishing campaigns: Top 10 targeted industries:

Accounting & Consulting
Wholesale Distribution
IT Services
Real Estate
Education
Healthcare
Chemicals
High Tech & Electronics
Legal Services
Outsourced Services

Up until a few years ago, cybercriminals focused their efforts on malware attacks for greatest ROI.

More recently, they've shifted their focus to phishing attacks with the goal of harvesting user credentials.

Is longer the better ?

Password Length	Possible Permutations	Time in seconds	Time in minutes	Time in hours	Time in days
6	782,757,789,696	8	0.13	0.002	0.00009
7	75,144,747,810,816	751	12.52	0.21	0.01
8	7,213,895,789,838,340	72,139	1,202.32	20.04	0.83
9	692,533,995,824,480,000	6,925,340	115,422.33	1,923.71	80.15
10	66,483,263,599,150,100,000	664,832,636	11,080,543.93	184,675.73	7,694.82

Hackers ♥ passwords

Most frequently rejected passwords from the just this last week

1	welc0me
2	2018
3	pa$$w0rd
4	1234
5	winter

6	fall
7	december
8	apple
9	soccer
10	bern

Is this password strong enough?

ji32k7au4a83

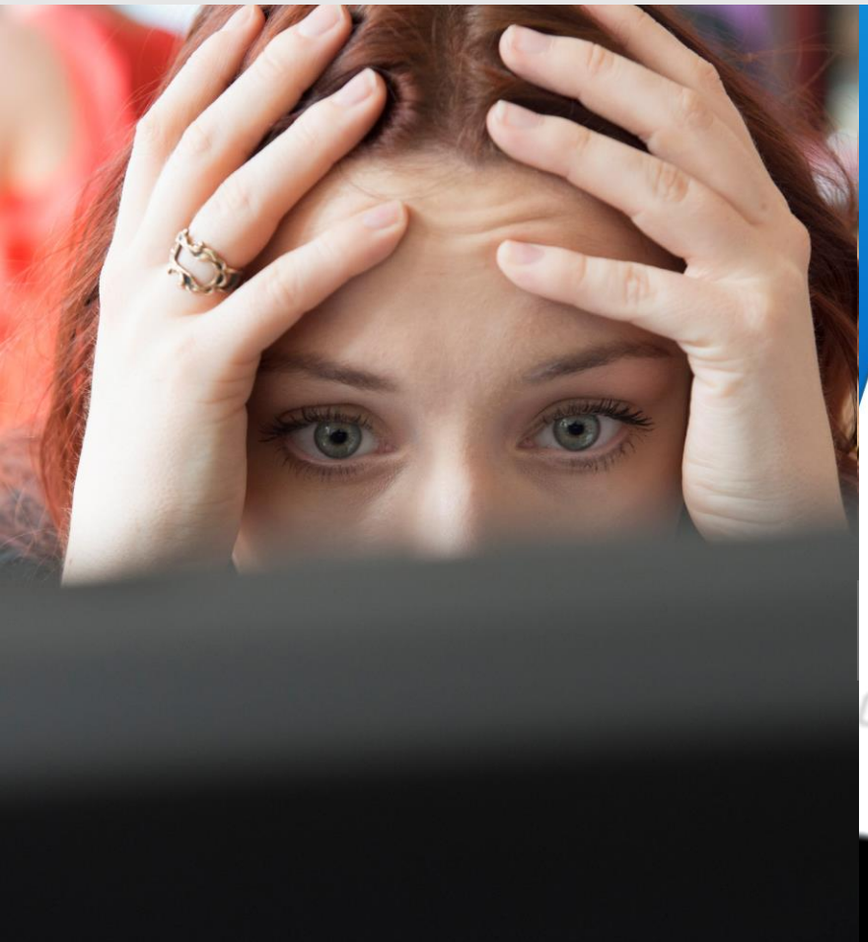
NO! It means “my password” in Chinese

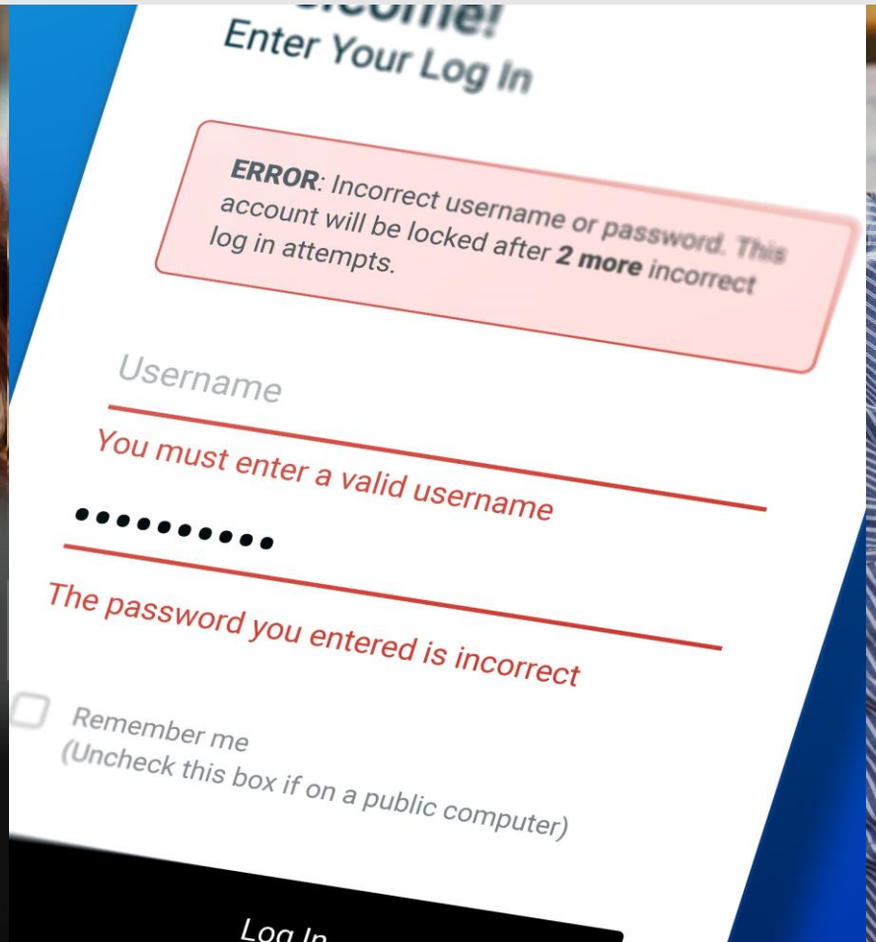
Users hate passwords

Alpha-numeric passwords are hard to remember

On mobile devices passwords are impossible to enter

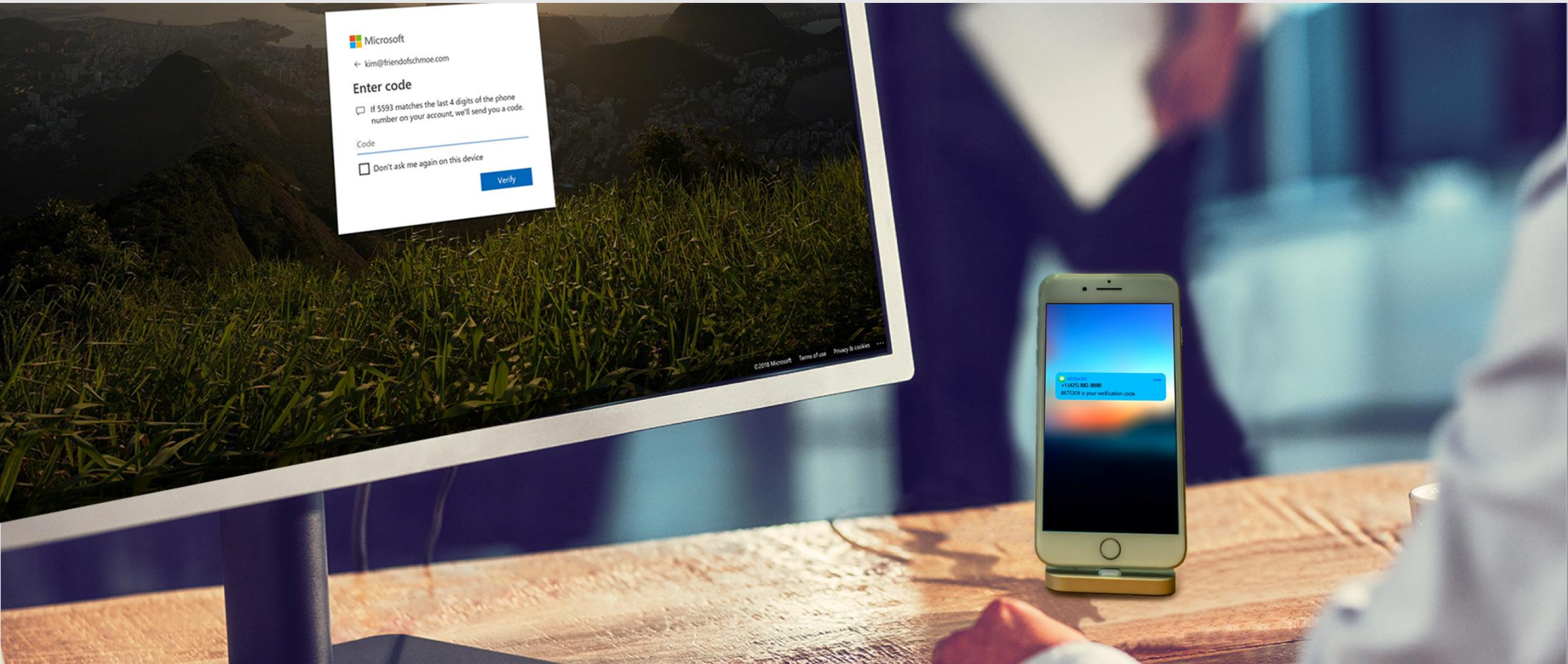
Password managers are not simple and only kind of work



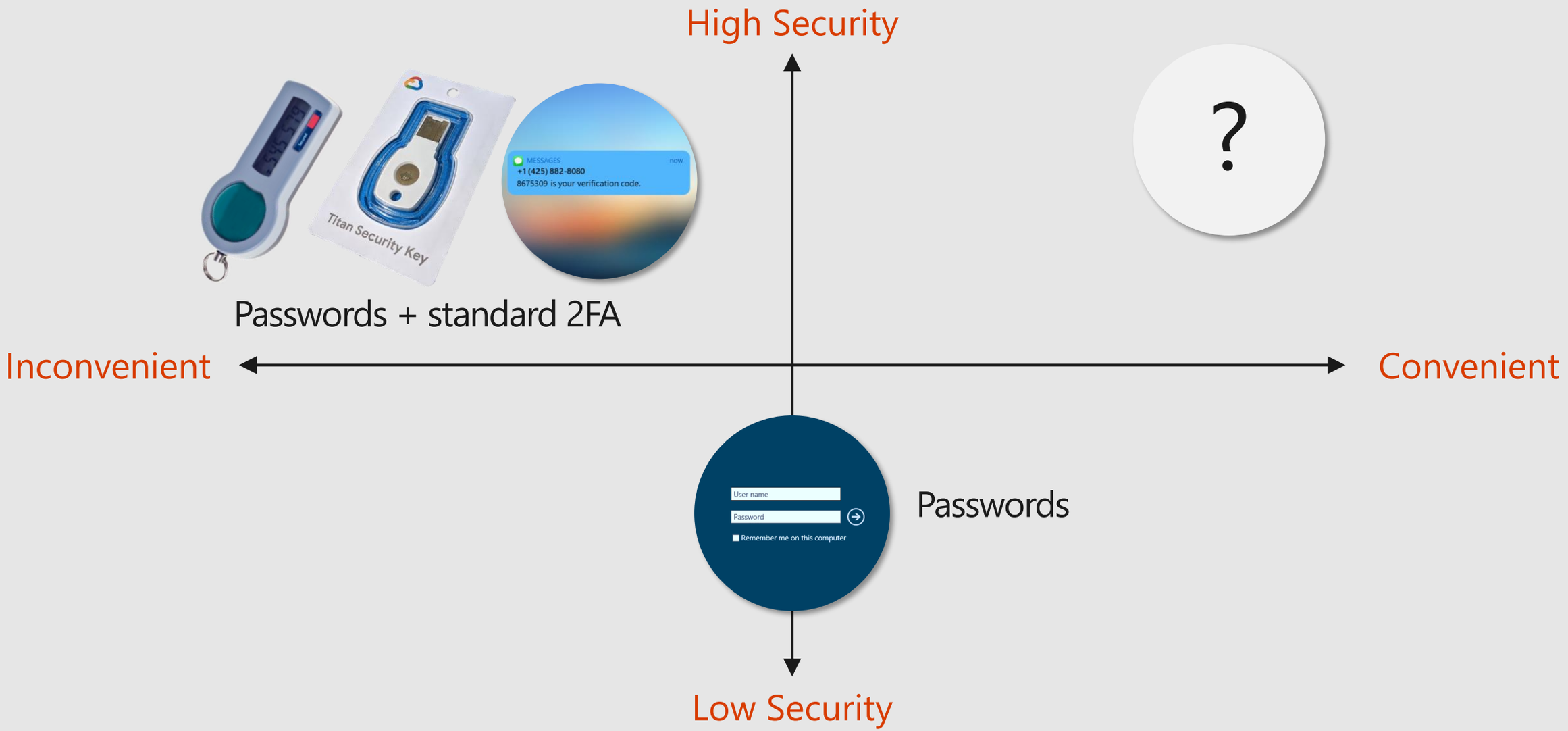


What about multi-factor authentication?

Passwords + MFA is more secure, but can also be more complicated to use.



There must be a better way

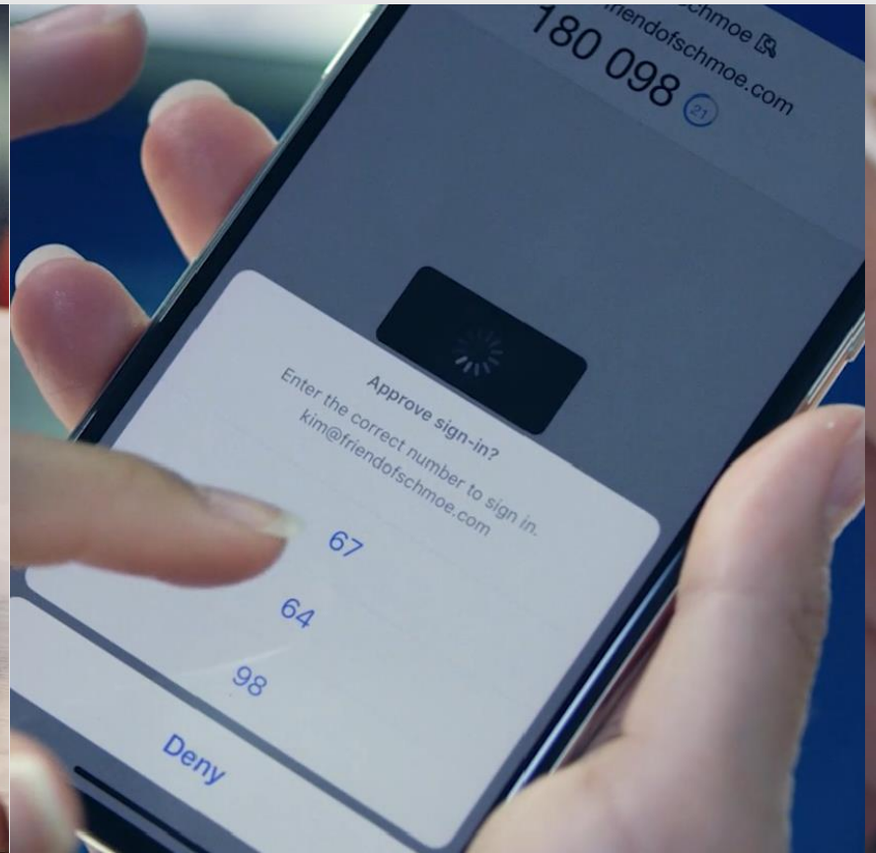


Password-free access to your apps

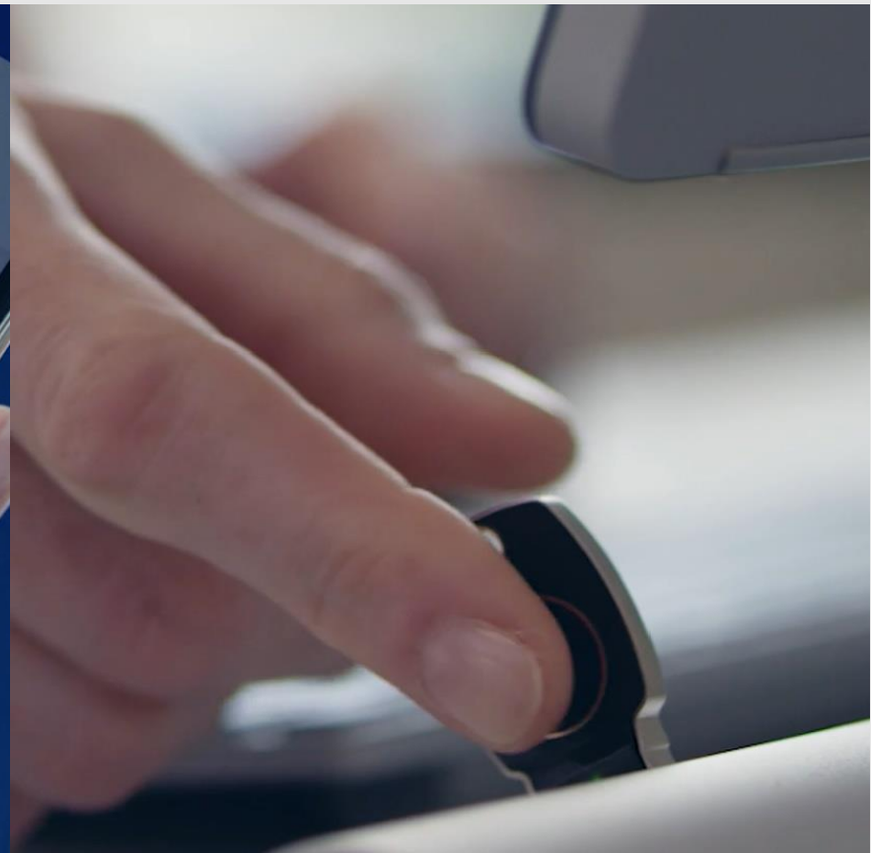
Help users keep their identities safe and give users more choice with standards-based password-less authentication

Windows Hello

Microsoft Authenticator



FIDO2 Security Keys



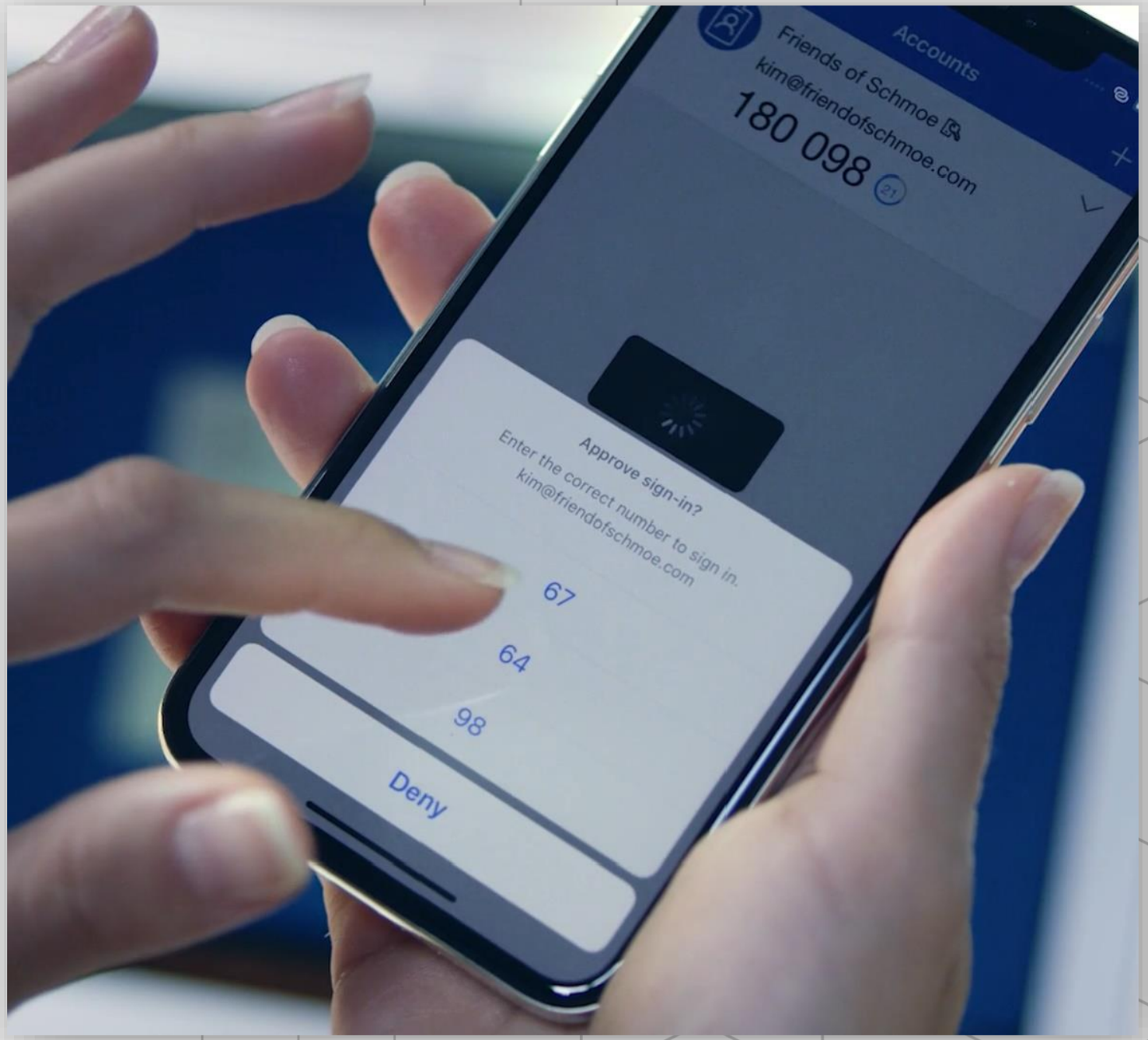
Windows Hello

Microsoft’s premier password-less experience

Microsoft Authenticator

Microsoft’s password-less anywhere solution

Azure Active Directory phone sign-in



Demo

Challenge with Multi-Factor Authentication, w/ Apple Watch and Terms of Use to an app when using a non-managed device

Chrome File Edit View History Bookmarks People Window Help

100% Sat Mar 2 7:54 PM

New Tab

mail.google.com/a/soseman.org

mail.google.com/a/soseman.org

mail.google.com/a/soseman.org - Google Search

You've gone incognito

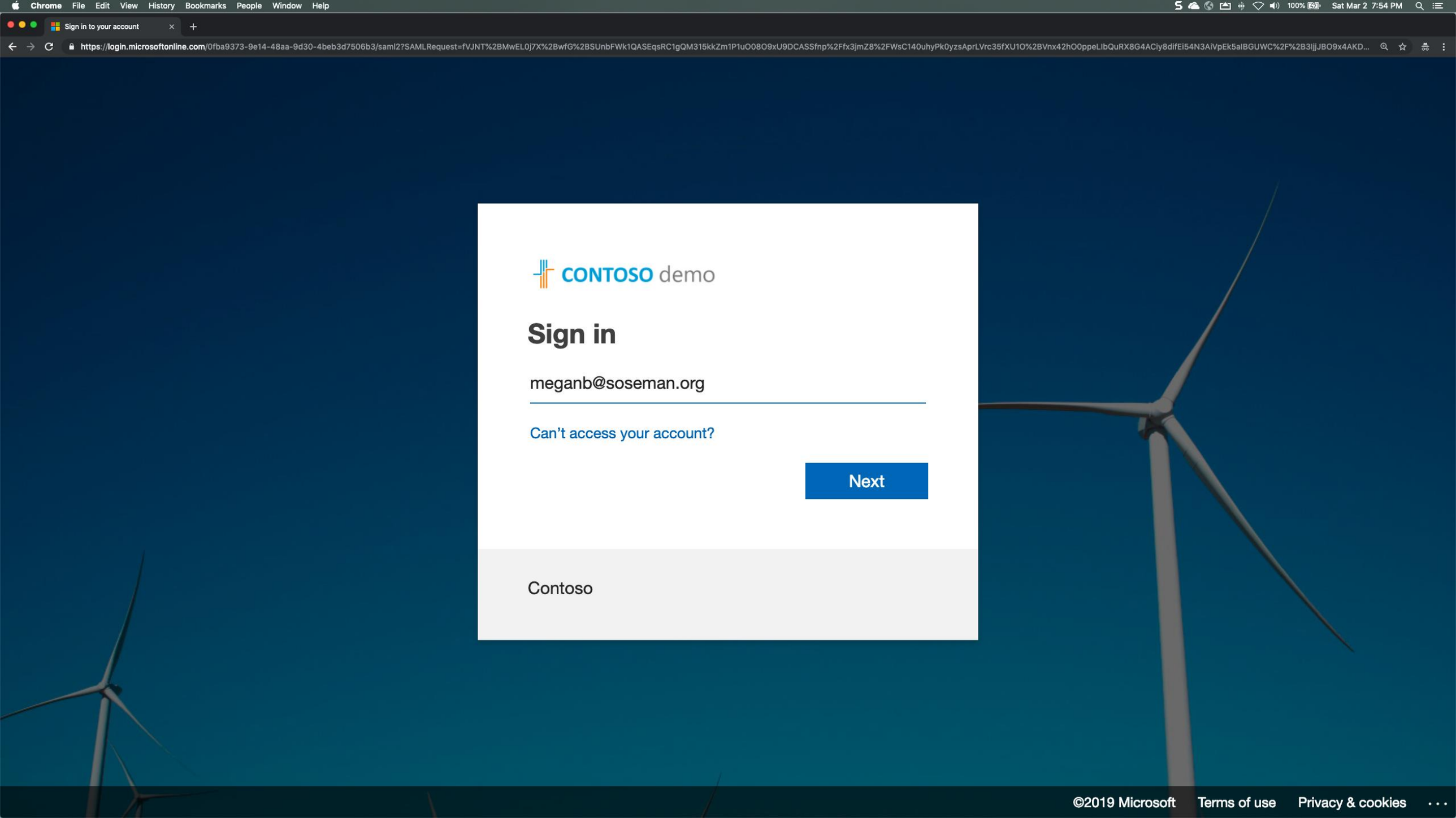
Now you can browse privately, and other people who use this device won't see your activity. However, downloads and bookmarks will be saved. Learn more

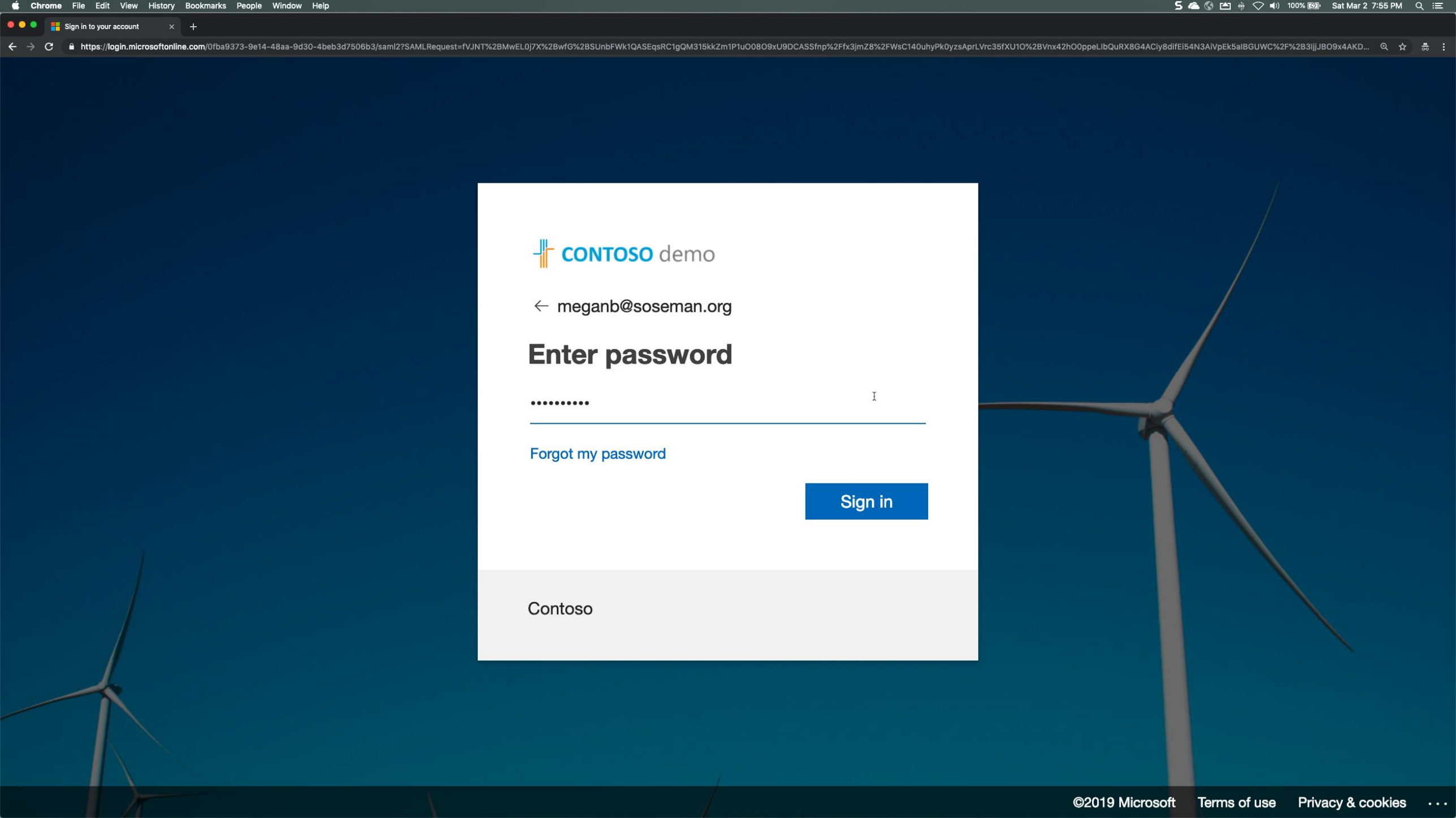
Chrome won't save the following information:

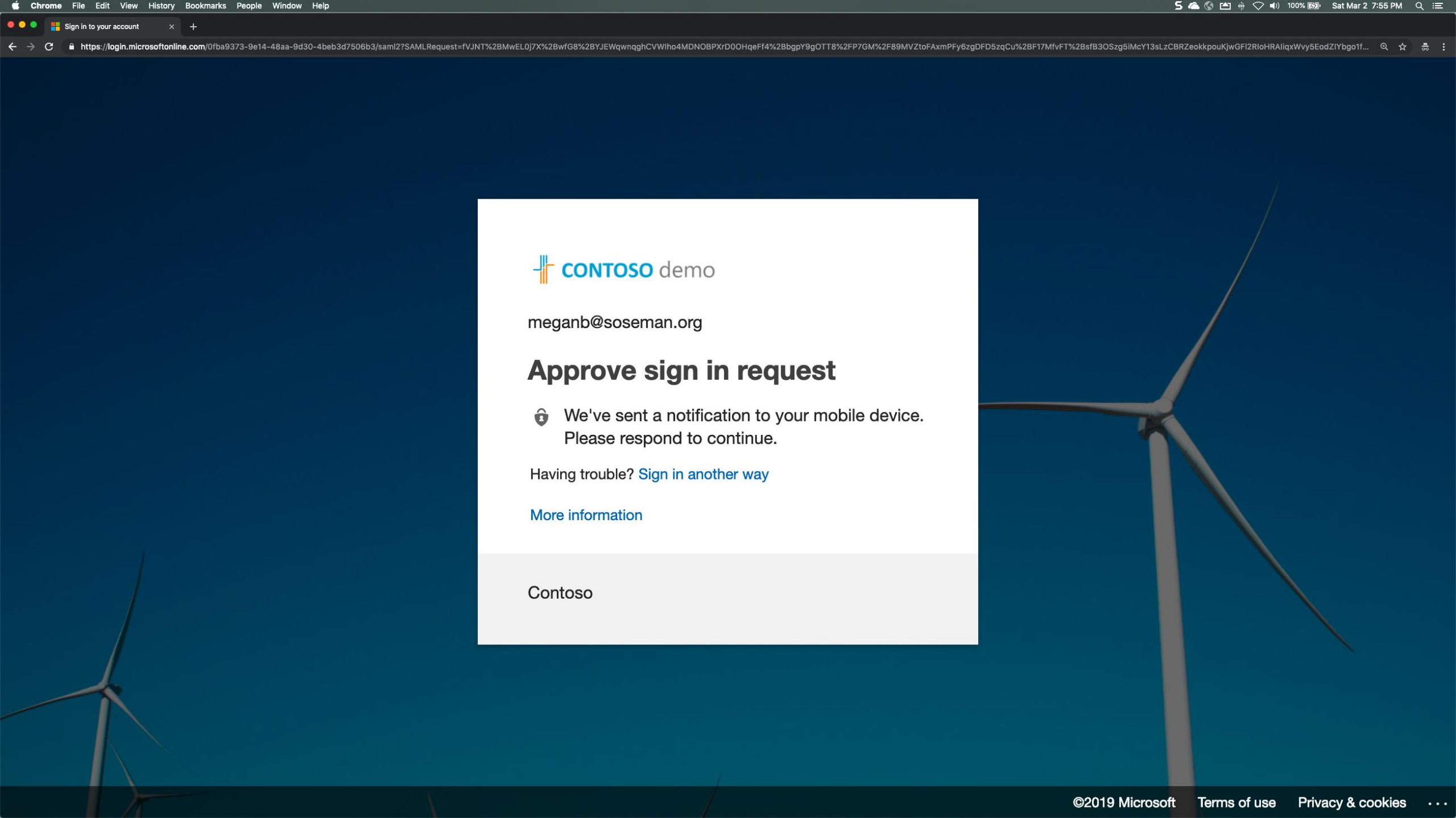
- Your browsing history
- Cookies and site data
- Information entered in forms

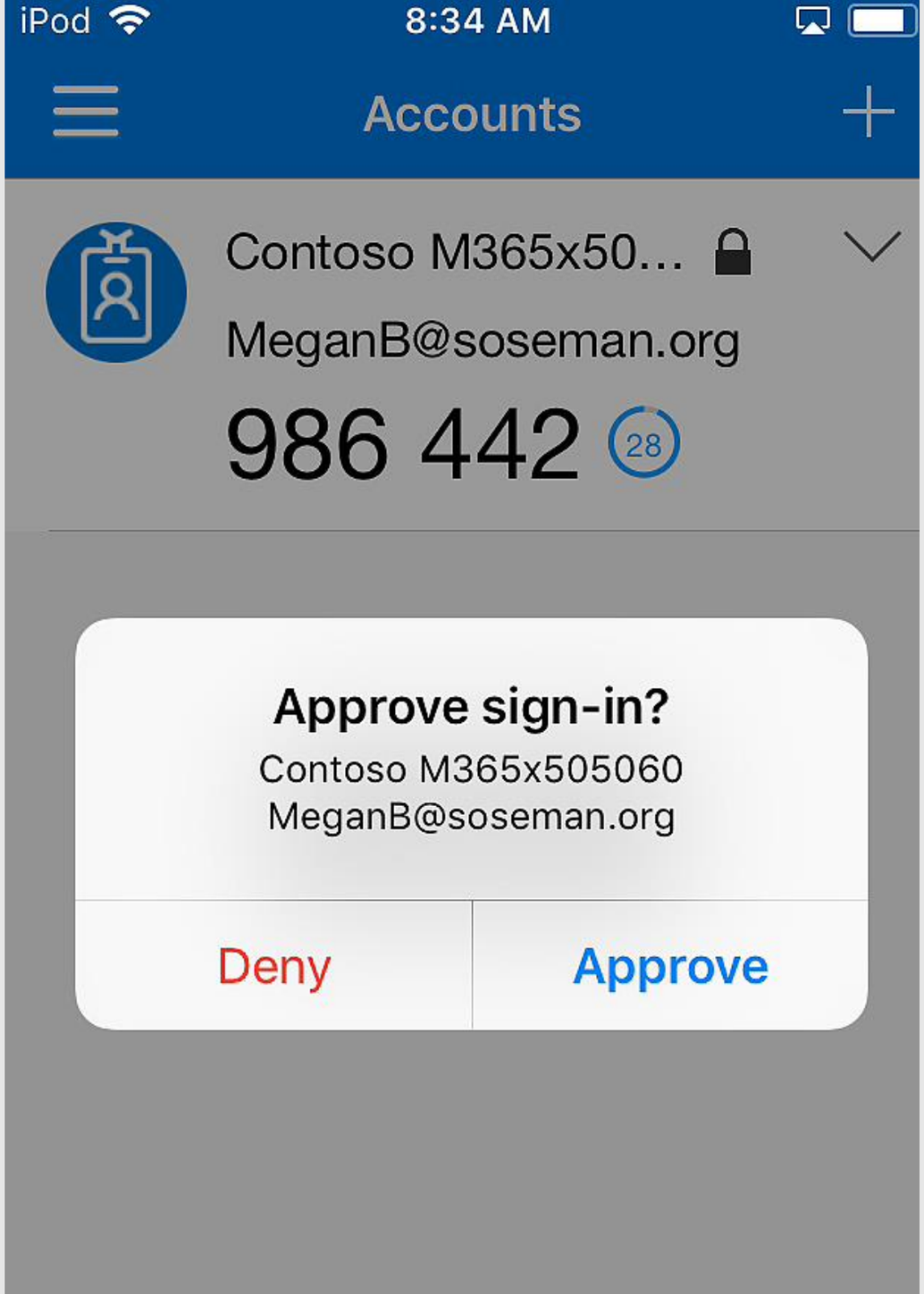
Your activity might still be visible to:

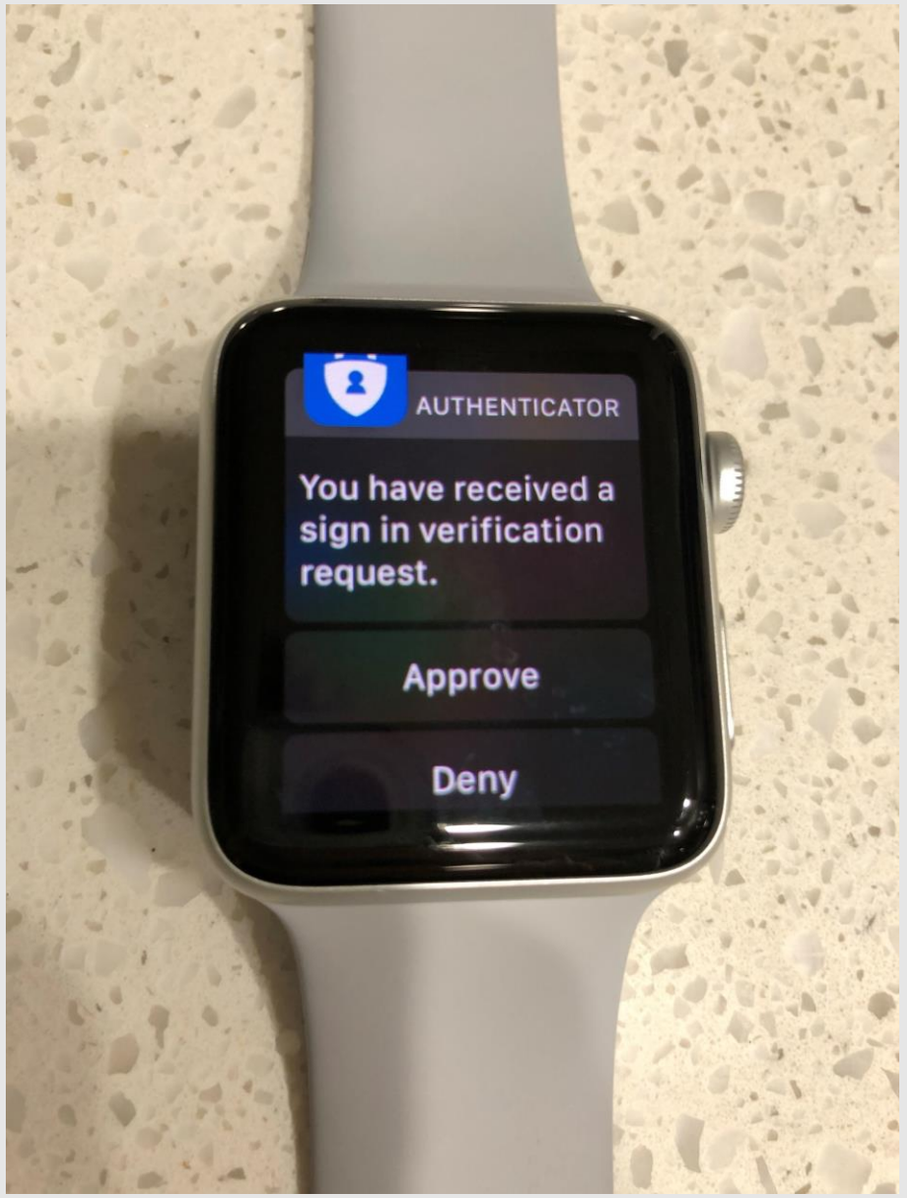
- Websites you visit
- Your employer or school
- Your internet service provider


Chrome File Edit View History Bookmarks People Window Help
100% Sat Mar 2 7:54 PM
Sign in to your account
https://login.microsoftonline.com/0fba9373-9e14-48aa-9d30-4beb3d7506b3/saml2?SAMLRequest=fVJNT%2BMwEL0j7X%2BwfG%2BSUnbFWk1QASEqsRC1gQM315kkZm1P1uO08O9xU9DCASSfnp%2Ffx3jmZ8%2FWsC140uhyPk0yzsAprLVrc35fXU1O%2BVnx42hO0ppeLIbQuRX8G4ACiy8difEi54N3AiVpEk5aIBGUWC%2F%2B3IjJBO9x4AKD...
CONTOSO demo
Sign in
meganb@soseman.org
Can’t access your account?
Next
Contoso
©2019 Microsoft
Terms of use
Privacy & cookies
• • •


Chrome File Edit View History Bookmarks People Window Help
100% Sat Mar 2 7:55 PM
Sign in to your account
https://login.microsoftonline.com/0fba9373-9e14-48aa-9d30-4beb3d7506b3/saml2?SAMLRequest=fVJNT%2BMwEL0j7X%2BwfG%2BSUnbFWk1QASEqsRC1gQM315kkZm1P1uO08O9xU9DCASSfnp%2Ffx3jmZ8%2FWsC140uhyPk0yzsAprLVrc35fXU1O%2BVnx42hO0ppeLIbQuRX8G4ACiy8difEi54N3AiVpEk5aIBGUWC%2F%2B3IjJBO9x4AKD...
CONTOSO demo
meganb@soseman.org
Enter password
Forgot my password
Sign in
Contoso
©2019 Microsoft
Terms of use
Privacy & cookies


Chrome File Edit View History Bookmarks People Window Help
Sat Mar 2 7:55 PM
Sign in to your account
https://login.microsoftonline.com/0fba9373-9e14-48aa-9d30-4beb3d7506b3/saml2?SAMLRequest=fVJNT%2BMwEL0j7X%2BwfG8%2BYJEWqwnqghCVWlho4MDNOBPXrD0OHqeFf4%2BbgpY9gOTT8%2FP7GM%2F89MVZtoFAxmPFy6zgDFD5zqCu%2BF17MfvFT%2BsfB3OSzg5iMcY13sLzCBRZeokkpouKjwGFl2RloHRAliqxWvy5EodZlYbgo1f...
CONTOSO demo
meganb@soseman.org
Approve sign in request
We've sent a notification to your mobile device.
Please respond to continue.
Having trouble? Sign in another way
More information
Contoso
©2019 Microsoft
Terms of use
Privacy & cookies


iPod
8:34 AM
Accounts
Contoso M365x50...
MeganB@soseman.org
986 442
28
Approve sign-in?
Contoso M365x505060
MeganB@soseman.org
Deny
Approve


AUTHENTICATOR
You have received a sign in verification request.
Approve
Deny

CONTOSO demo

Contoso terms of use

In order to access Contoso resource, you must read the terms of use.

Terms of Use >

Please click Accept to confirm that you have read and understood the terms of use.

Decline **Accept**

Password-less with FIDO2 security keys

Microsoft uses open standards that work with innovative offerings from partners

USB/NFC Key

USB Biometric Key

Biometric Wearables

';--have i been pwned?

Check if your email or phone is in a data breach

email or phone (international format) pwned?

550	11,420,802,014	114,115	202,459,541
pwned websites	pwned accounts	pastes	paste accounts

Largest breaches

772,904,991 Collection #1 accounts

763,117,241 Verifications.io accounts

711,477,622 Onliner Spambot accounts

622,161,052 Data Enrichment Exposure From

Recently added breaches

2,743,539 Audi accounts

112,031 Guntrader accounts

505,466 Short Édition accounts

30,433 Vastaamo accounts

https://haveibeenpwned.com

Home | Notify me | Domain search | Who's been pwned | Passwords | API | About

';--have i been pwned?

Check if your email or phone is in a data breach

abbas.kudrati@microsoft.com

Oh no — pwned!

Pwned in 1 data breach and found no pastes (subscribe to search sensitive breaches)

Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the 1Password password manager helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.

Data Enrichment Exposure From PDL Customer: In October 2019, security researchers Vinny Troia and Bob Diachenko identified an unprotected Elasticsearch server holding 1.2 billion records of personal data. The exposed data included an index indicating it was sourced from data enrichment company People Data Labs (PDL) and contained 622 million unique email addresses. The server was not owned by PDL and it's believed a customer failed to properly secure the database. Exposed information included email addresses, phone numbers, social media profiles and job history data.

Compromised data: Email addresses, Employers, Geographic locations, Job titles, Names, Phone numbers, Social media profiles

Canva: In May 2019, the graphic design tool website Canva suffered a data breach that impacted 137 million subscribers. The exposed data included email addresses, usernames, names, cities of residence and passwords stored as bcrypt hashes for users not using social logins. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".

Compromised data: Email addresses, Geographic locations, Names, Passwords, Usernames

Cit0day (unverified): In November 2020, a collection of more than 23,000 allegedly breached websites known as Cit0day were made available for download on several hacking forums. The data consisted of 226M unique email address alongside password pairs, often represented as both password hashes and the cracked, plain text versions. Independent verification of the data established it contains many legitimate, previously undisclosed breaches. The data was provided to HIBP by dehashed.com.

Compromised data: Email addresses, Passwords

Collection #1 (unverified): In January 2019, a large collection of credential stuffing lists (combinations of email addresses and passwords used to hijack accounts on other services) was discovered being distributed on a popular hacking forum. The data contained almost 2.7 *billion* records including 773 million unique email addresses alongside passwords those addresses had used on other breached services. Full details on the incident and how to search the breached passwords are provided in the blog post The 773 Million Record "Collection #1" Data Breach.

Compromised data: Email addresses, Passwords

Data & Leads: In November 2018, security researcher Bob Diachenko identified an unprotected database believed to be hosted by a data aggregator. Upon further investigation, the data was linked to marketing company Data & Leads. The exposed Elasticsearch instance contained over 44M unique email addresses along with names, IP and physical addresses, phone numbers and employment information. No response was received from Data & Leads when contacted by Bob and their site subsequently went offline.

Compromised data: Email addresses, Employers, IP addresses, Job titles, Names, Phone numbers, Physical addresses

Exploit.In (unverified): In late 2016, a huge list of email address and password pairs appeared in a "combo list" referred to as "Exploit.In". The list contained 593 million unique email addresses, many with multiple different passwords hacked from various online systems. The list was broadly circulated and used for "credential stuffing", that is attackers employ it in an attempt to identify other online systems where the account owner had reused their password. For detailed background on this incident, read Password reuse, credential stuffing and another billion records in Have I Been Pwned.

Compromised data: Email addresses, Passwords

Lead Hunter: In March 2020, a massive trove of personal information referred to as "Lead Hunter" was provided to HIBP after being found left exposed on a publicly facing Elasticsearch server. The data contained 69 million unique email addresses across 110 million rows of data accompanied by additional personal information including names, phone numbers, genders and physical addresses. At the time of publishing, the breach could not be attributed to those responsible for obtaining and exposing it. The data was provided to HIBP by dehashed.com.

Compromised data: Email addresses, Genders, IP addresses, Names, Phone numbers, Physical addresses

Nitro: In September 2020, the Nitro PDF service suffered a massive data breach which exposed over 70 million unique email addresses. The breach also exposed names, bcrypt password hashes and the titles of converted documents. The data was provided to HIBP by dehashed.com.

Compromised data: Email addresses, Names, Passwords

Onliner Spambot (spam list): In August 2017, a spambot by the name of Onliner Spambot was identified by security researcher Benkow moqu3q. The malicious software contained a server-based component located on an IP address in the Netherlands which exposed a large number of files containing personal information. In total, there were 711 million unique email addresses, many of which were also accompanied by corresponding passwords. A full write-up on what data was found is in the blog post titled Inside the Massive 711 Million Record Onliner Spambot Dump.

Compromised data: Email addresses, Passwords

River City Media Spam List (spam list): In January 2017, a massive trove of data from River City Media was found exposed online. The data was found to contain almost 1.4 billion records including email and IP addresses, names and physical addresses, all of which was used as part of an enormous spam operation. Once de-duplicated, there were 393 million unique email addresses within the exposed data.

Compromised data: Email addresses, IP addresses, Names, Physical addresses

SC Daily Phone Spam List (spam list): In early 2015, a spam list known as SC Daily Phone emerged containing almost 33M identities. The data includes personal attributes such as names, physical and IP addresses, genders, birth dates and phone numbers. Read more about spam lists in HIBP.

Compromised data: Dates of birth, Email addresses, Genders, IP addresses, Names, Physical addresses

Scentbird: In June 2020, the online fragrance service Scentbird suffered a data breach that exposed the personal information of over 5.8 million customers. Personal information including names, email addresses, genders, dates of birth, passwords stored as bcrypt hashes and indicators of password strength were all exposed. The data was provided to HIBP by breachbase.pw.

https://haveibeenpwned.com

Home | Notify me | Domain search | Who's been pwned | Passwords | API | About | Donate

';--have i been pwned?

Check if your email or phone is in a data breach

abbask@gmail.com pwned?

Oh no — pwned!

Pwned in 14 data breaches and found no pastes (subscribe to search sensitive breaches)

Exploit.In (unverified): In late 2016, a huge list of email address and password pairs appeared in a "combo list" referred to as "Exploit.In". The list contained 593 million unique email addresses, many with multiple different passwords hacked from various online systems. The list was broadly circulated and used for "credential stuffing", that is attackers employ it in an attempt to identify other online systems where the account owner had reused their password. For detailed background on this incident, read Password reuse, credential stuffing and another billion records in Have I Been Pwned.

Compromised data: Email addresses, Passwords

Lead Hunter: In March 2020, a massive trove of personal information referred to as "Lead Hunter" was provided to HIBP after being found left exposed on a publicly facing Elasticsearch server. The data contained 69 million unique email addresses across 110 million rows of data accompanied by additional personal information including names, phone numbers, genders and physical addresses. At the time of publishing, the breach could not be attributed to those responsible for obtaining and exposing it. The data was provided to HIBP by dehashed.com.

Compromised data: Email addresses, Genders, IP addresses, Names, Phone numbers, Physical addresses

Nitro: In September 2020, the Nitro PDF service suffered a massive data breach which exposed over 70 million unique email addresses. The breach also exposed names, bcrypt password hashes and the titles of converted documents. The data was provided to HIBP by dehashed.com.

Compromised data: Email addresses, Names, Passwords

Onliner Spambot (spam list): In August 2017, a spambot by the name of Onliner Spambot was identified by security researcher Benkow moqu3q. The malicious software contained a server-based component located on an IP address in the Netherlands which exposed a large number of files containing personal information. In total, there were 711 million unique email addresses, many of which were also accompanied by corresponding passwords. A full write-up on what data was found is in the blog post titled Inside the Massive 711 Million Record Onliner Spambot Dump.

Compromised data: Email addresses, Passwords

River City Media Spam List (spam list): In January 2017, a massive trove of data from River City Media was found exposed online. The data was found to contain almost 1.4 billion records including email and IP addresses, names and physical addresses, all of which was used as part of an enormous spam operation. Once de-duplicated, there were 393 million unique email addresses within the exposed data.

Compromised data: Email addresses, IP addresses, Names, Physical addresses

SC Daily Phone Spam List (spam list): In early 2015, a spam list known as SC Daily Phone emerged containing almost 33M identities. The data includes personal attributes such as names, physical and IP addresses, genders, birth dates and phone numbers. Read more about spam lists in HIBP.

Compromised data: Dates of birth, Email addresses, Genders, IP addresses, Names, Physical addresses

Scentbird: In June 2020, the online fragrance service Scentbird suffered a data breach that exposed the personal information of over 5.8 million customers. Personal information including names, email addresses, genders, dates of birth, passwords stored as bcrypt hashes and indicators of password strength were all exposed. The data was provided to HIBP by breachbase.pw.

Microsoft

Q & A

Thank you

https://aka.ms/abbas