Cybersecurity is a solved problem

so uh ... why are breaches still happening?

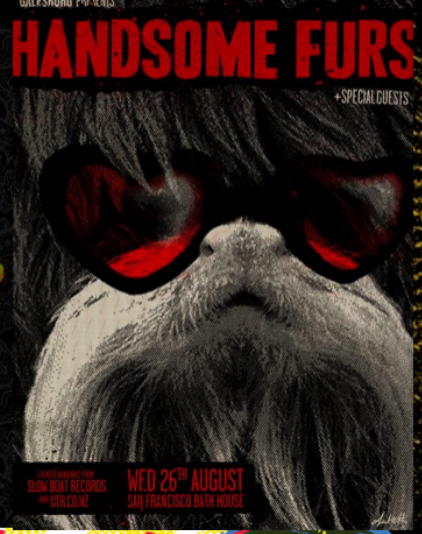
whoami

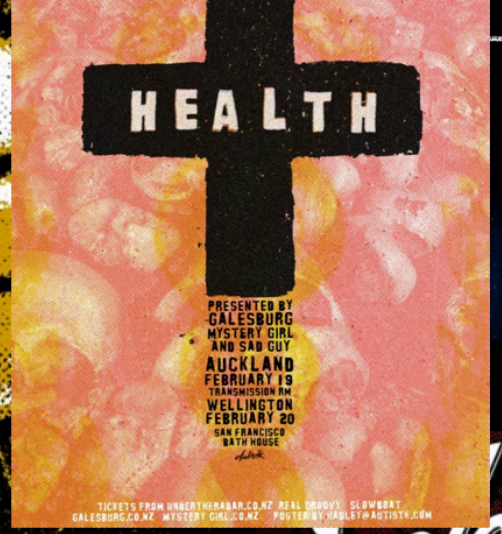
- I was a software developer, once
- Principal Security Consultant / Pentester @ Tier Zero
- DEFCON 32 speaker 2024 / security researcher
    - CVE-2024-38200 - MS Outlook and MS Office
    - CVE-2024-38020 - MS Outlook
- MSRC bug bounty leaderboard Q1 and Q2 2024
- Off By One speaker 2025 (Singapore)

HOMES.CO.NZ

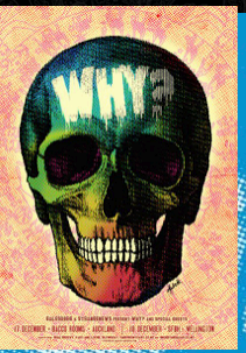
PRIVSECCONSULTING


GALESBURG PRESENTS
HOLY FUCK
SAN FRANCISCO BATH HOUSE
MONDAY DECEMBER 15 2008
TICKETS FROM SLOWBOAT RECORDS
or WWW.UTR.CO.NZ POSTER BY


HANDSOME FURS
+SPECIAL GUESTS
WED 26TH AUGUST
SAN FRANCISCO BATH HOUSE


HEALTH
PRESENTED BY
GALESBURG
MYSTERY GIRL
AND SAD GUY
AUCKLAND
FEBRUARY 19
TRANSMISSION ON
WELLINGTON
FEBRUARY 20
SAN FRANCISCO
BATH HOUSE


DEERHUNTER
PRESENTED BY: GALESBURG
DATE: TUESDAY SIXTEENTH JUNE 2009
VENUE: SAN FRANCISCO BATH HOUSE, CUBA ST

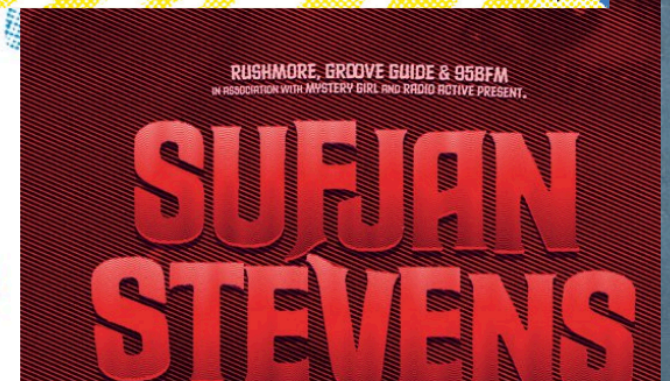

WHY?


GALESBURG PRESENTS
GIRL TALK
WITH SUPPORT FROM DROPKICK COUSINS
24 JANUARY 2009 SAN FRANCISCO BATH HOUSE
TICKETS FROM SLOWBOAT RECORDS AND UTR.CO.NZ


the National
TUE 15 JAN 08 AT THE KINGS ARMS IN AUCKLAND
WITH THE VIETNAM WAR AND GUESTS


galesburg and strangenews present
Explosions in the Sky
with Eluvium (usa) and guests
Mon February 11 Auckland Kings Arms
Tues February 12 Wellington San Francisco Bath House


Galesburg
95FM
PRESENT
PAVEMENT
1ST MARCH 2010 - AUCKLAND TOWN HALL
TICKETS FROM TICKETEK WWW.TICKETEK.CO.NZ WWW.MYSTERYGIRL.CO.NZ WWW.GALESBURG.CO.NZ


RUSHMORE, GROOVE GUIDE & 95BFM
IN ASSOCIATION WITH MYSTERY GIRL AND RADIO ACTIVE PRESENT.
SUFJAN STEVENS


GALESBURG and STRANGENEWS present
BROKEN SOCIAL SCENE
95FM
AUCKLAND WED FEBRUARY 20th WELLINGTON THURS FEBRUARY 21st
TICKETS AVAILABLE FROM REAL CROOVY (AUCKLAND) and SLOW BOAT RECORDS (WELLINGTON)
Cheese on Toast


RUSHMORE AND UNDER THE RADAR PRESENTS
LES Savy FAV
TUES 1 FEB, KINGS
WED 2 FEB, SFBH
TICKETS FROM SLOW BOAT RECORDS.

LIGHTNING BOLT

disclaimer

- some of the techniques you see are illegal, without prior consent
- there are safe places to practice:
  - PentesterLab
  - Hack The Box
  - Bug Bounty Programs (read the rules and stay in scope)

why this talk

- the NCSC estimated that the total loss to NZ in 2024 from cybercrime was 1.6 billion
- In the 2024/2025 financial year:
  - 5995 reports were recieved to the NCSC
  - 331 were triaged as having 'national significance' which meant extra support
- New Zealand's Cyber Security Strategy 2026-2030 was released in Feb:
  - a good blueprint for collective action against threats, worth a read!
  - https://www.dpmc.govt.nz/our-programmes/national-security/cyber-security-strategy

the outcomes of cybercrime are varied

- frequently it results in theft/exfiltration of 'personal information'
- can be extremely damaging, both to individuals and organisations
- sometimes it's economic, business disruption, destruction of data...

but haven't we solved this already?

- yes? no? maybe?
- we have a lot of things that can help us
- but there are a lot of reasons that they don't get implemented

what we're going to talk about

- some shared definitions
- the essential 8 (yay) - mitigation strategies
  - NZ has NCSC Critical Controls which overlap
- how breaches can happen
- what low friction security controls we have to prevent it
- why it's hard and what change can look like in your organisation

what this isn't

- a cybersecurity professional telling you to simply fix all the things
  - the industry has enough people trying to beat you over the head with the cyber stick
  - the best outcomes come from collectively learning and fixing together
- the sky is falling because of AI (it's not)
- "XYZ tool would have solved ABC data breach"

some shared definitions:

- Tactics, Techniques, and Procedures (TTP)
- Advanced Persistent Threat (APT)
- Zero day: an unknown vulnerability that does not have a fix
- Common Vulnerabilities and Exposures (CVE)

more definitions

- workstation: someones device like a laptop
- internet facing server: another computer that has some things exposed on the internet
- sandbox: a way of keeping programs separate.
    - browsers are pretty well sandboxed
- powershell: a clackity clackity interface that allows for programmatic interaction with a computer

unto the breach

- Data breach
  - Help someone has stolen data
- Confidentiality breach
  - Help someone has stolen secret data
- Privacy breach
  - Help someone has stolen personal data

sensitive data/information

- sensitive personal information (thanks OPC ❤️)

> Sensitive personal information is information about the individual that has some real significance to them, is revealing of them, or generally relates to matters that an individual might wish to keep private.

- this is largely what we want to keep safe and secure

the essential 8:

- patch applications
- patch operating systems
- **multi-factor authentication** ❤️
- restrict administrative privileges ❤️
- application control ❤️
- restrict Microsoft Office macros ❤️
- user application hardening
- regular backups

the essential 8 is...

- a baseline, designed to help secure systems
- mitigations for common security issues that can make it hard for a threat actor to do things
- clear practical steps that an organisation can take to help secure their stuff
- made up of different maturity levels for a range of organisations

the essential 8 is not...

- a definitive and final plan
- a recommendation for any specific product or service
  - organisations will have to make their own decisions about what is appropriate

a note about users

- end users are frequently cited as taking risky actions which result in compromise
  - they clicked a link! bad user!
- it is the job of the security practitioner to fix this for the user
- give them guardrails, give them protections that help keep them safe, give them an easy secure path

pinning breaches on 'human error' is incredibly disingenuous

> 'Human error was a major contributing cause in 95% of all breaches.' — IBM Cyber Security Intelligence Index Report.

- have you tried designing systems resistant to human error???

a note about measuring change

- you might do all the things, but traditional security metrics can make it hard to measure whether the change has been effective
- reasons breaches/security events don't happen:
  - people don't do cybercrime against you
  - people do cybercrime against you but the security controls are effective

unsafe at any speed

The Designed-In Dangers of the American Automobile

- written by consumer advocate Ralph Nader in the 1960's
- car manufacturers were generally reluctant to spend money on improving safety
- Nader argued that cars were designed in ways that made them inherently dangerous, and that safety features were ignored in favor of styling and cost-cutting :"user experience"
- the book resulted in the creation of the United States Department of Transportation

UNSAFE AT ANY SPEED

The Designed-In Dangers of The American Automobile

By Ralph Nader

sound familiar?

- Chapter 7: "Damn the driver and spare the car"
- discusses the "way vehicular crashes and harm was placed on the driver."
- alleges that "Engineering, Enforcement and Education" was created by the industry
- "Enforcement and Education" meant the driver
- "Engineering" was all about the road
- maybe the author of that IBM report should read this

tech and security is having a slow realisation that we have been here before

- one of the favourite pastimes of tech people is reinventing things that already exists
- see elon musk and the train
- cybersecurity can and should learn from other industries

How breaches happen, at a high level

- ClickFix
- Phishing
- malicious documents
- other breaches/password reuse

wtf is clickfix

- a technique that tricks users into running commands
  - turns out computers can do that
- "Verify you are human"
- can be a fake CAPTCHA, browser, system errors, windows update

Verification Steps

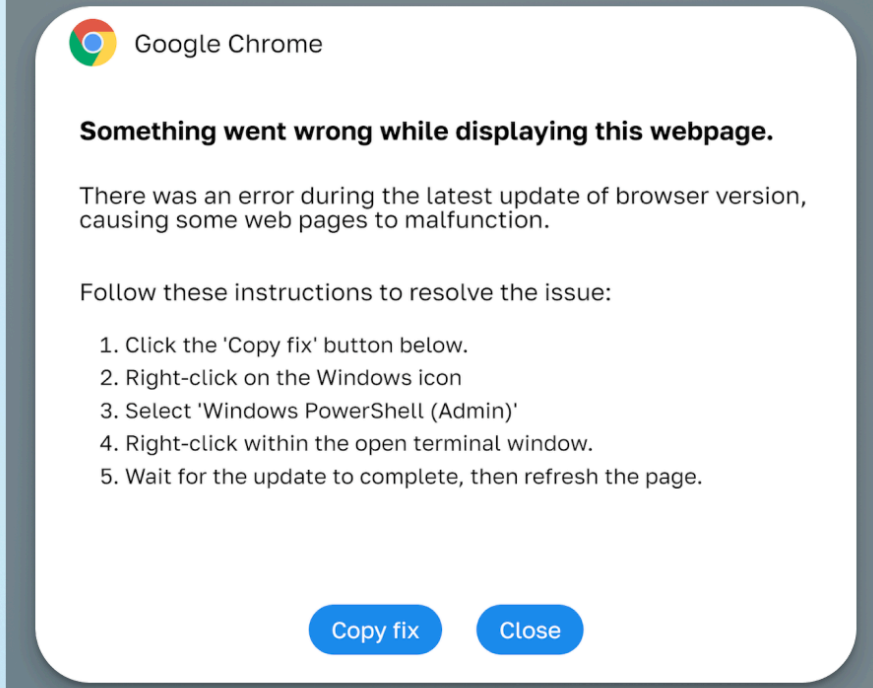
1. Press Windows Button "⊞" + R
2. Press CTRL + V
3. Press Enter

Follow 3 steps for verification

Step 1: Press Windows Button"⊞" + R

Step 2: Press CTRL V

Step 3: Press Enter



what happens

- JavaScript (the scripting language that runs in a browser) silently copies the naughty thing to the clipboard
- the screen says: `Hit Win+R then Ctrl-V`
    - Win+R is the run window
- varying degrees of fun things happen to your computer

like..

- malware
- Remote Access Trojans
    - allows for full computer control
- infostealers
    - steal browser credentials, saved credentials and other things
- ✨ ransomware ✨

ok but how do i (or a security team) prevent this?

- essential 8 recommends "application control"
- this can mean:
  - restricting Win+R run dialog
  - restricting PowerShell
- most normal users won't need this things! honestly!
- the average sysadmin has the ability to disable these things for users

phishing🐟

- an old favourite of all sorts of threat actors
- from serious ransomware operators to spam generators
- user clicks a link
    - like i mentioned, browsers are frequently sandboxed
- the bad thing happens when a user gives over their credentials

ah but I have MFA

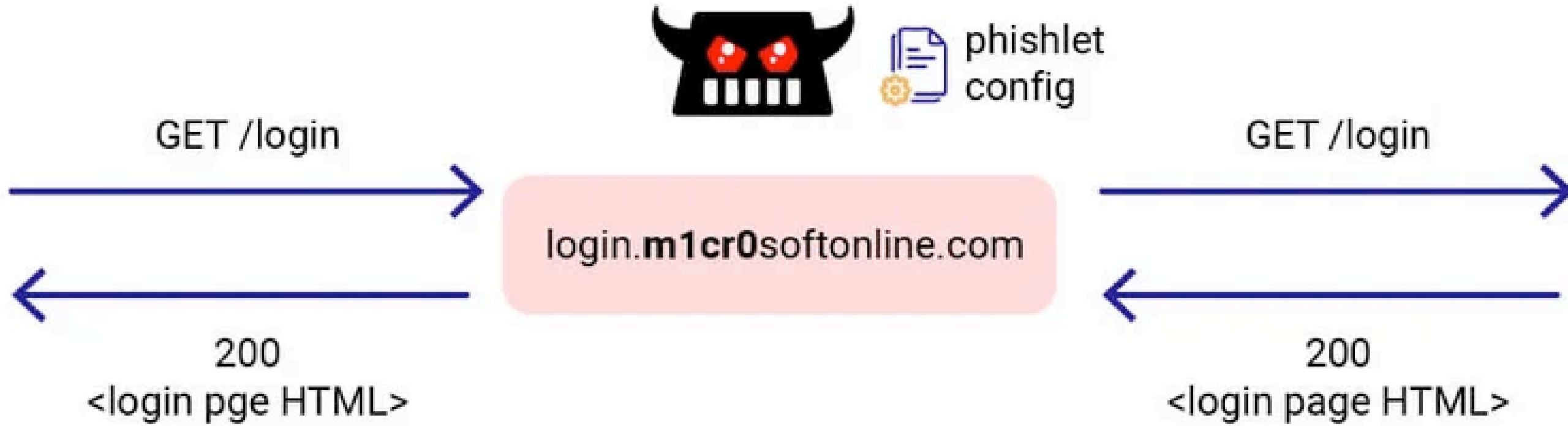
- well, some MFA is phishable (and some is phishing resistant - we'll get to that)
- serious phishing attempts using a transparent proxy
- allows for a Person in The Middle (PitM) attack
- MFA tokens can also be stolen and relayed directly to the legitimate service (OWA, Azure etc)

evil nginx

- nginx is a server
- evil nginx is...the evil version?
    - used to proxy/forward requests between users and legitimate servers
- what even is the point of making a tool if you can't make a cool logo

pitm

- a classic person in the middle attack
- someone sends link
- user clicks link
- enters credentials
    - and enters OTP!
- credentials and token are proxied / forwarded to legitimate service
- session generated and captured by hackeroo


phishlet
config
GET /login
GET /login
login.m1cr0softonline.com
200
<login pge HTML>
200
<login page HTML>

what even is MFA

- two or more of the following:
  - something you know (a password, pin or passphrase)
  - something you have (a security key, a passcard, a one time password, a smartphone)
  - something you are, such as your face geometry or fingerprint.

not all MFA are created equal

- MFA tokens can be phished, as we discovered
- some, like those from hardware tokens (little devices that plug into USB) are 'phishing resistant'
- let's see how that works!

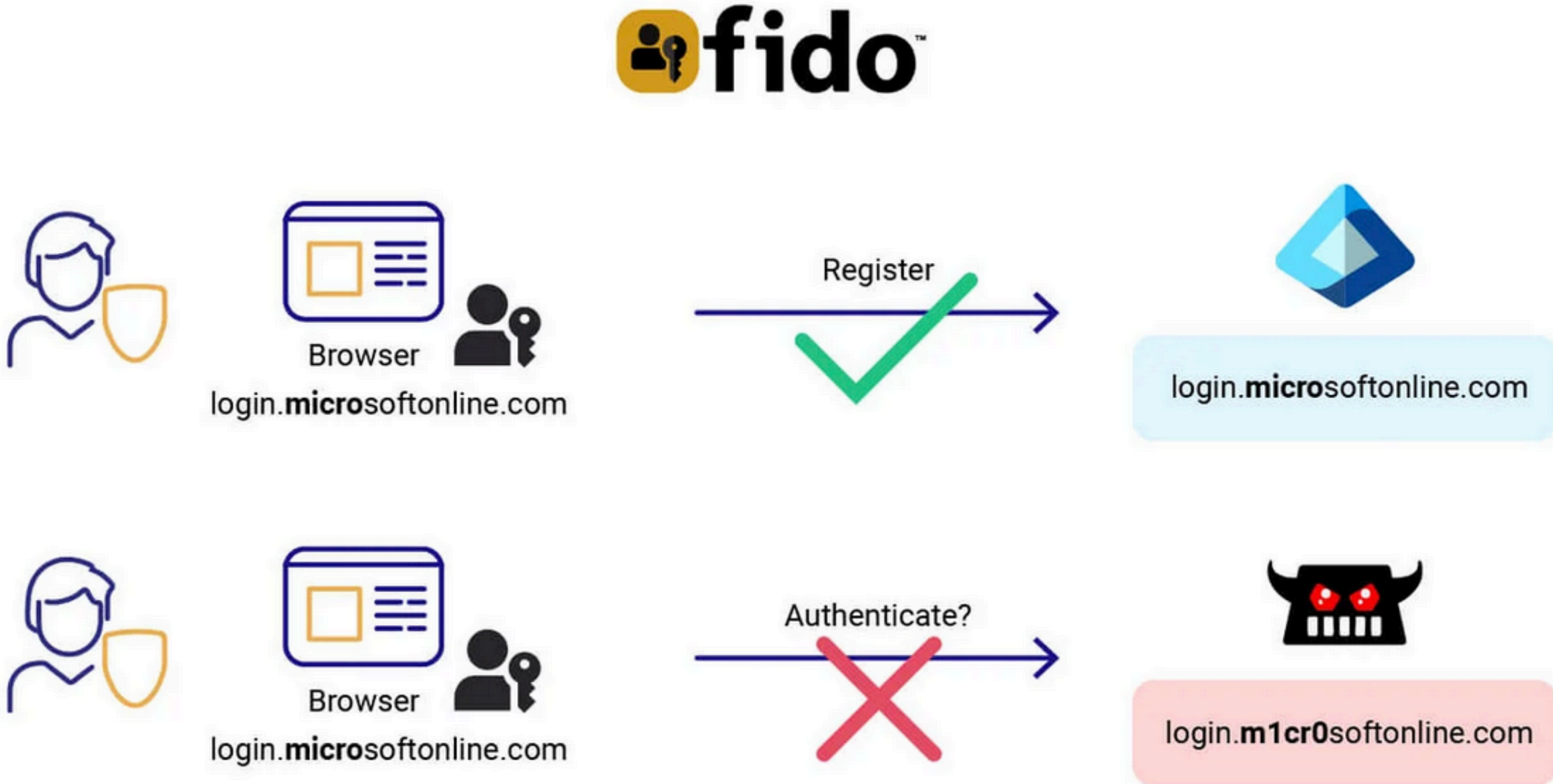
FIDO

> open, phishing-resistant authentication protocols developed by the FIDO Alliance to eliminate over-reliance on passwords.

- uses public key cryptography!
- tl;dr private and public key:
  - public key is designed to be shared
  - no issues if someone finds it!
  - robust and battle tested

another cool thing about this protocol

- the protocol/factor is 'bound' to the site/URL
- if a user is phished, and tries to enter credentials to a fraudulent site?


fido
Browser
login.microsoftonline.com
Register
login.microsoftonline.com
Browser
login.microsoftonline.com
Authenticate?
login.m1cr0softonline.com

we can remove passwords altogether

- passwords have been known to be an incredibly weak link for years
- even MS has 'Windows Hello'
  - replaces password with "something you have" (the device)
  - and "something you are" (biometrics)
  - or "something you know" (PIN).
  - surprisingly effective
- a good example of an easy & secure path

passkeys are also good option

- built on "public key cryptography" also
- made up of the "public key"
    - which is stored by the website
- and the private key
    - which is stored on your device

passkeys (continued)

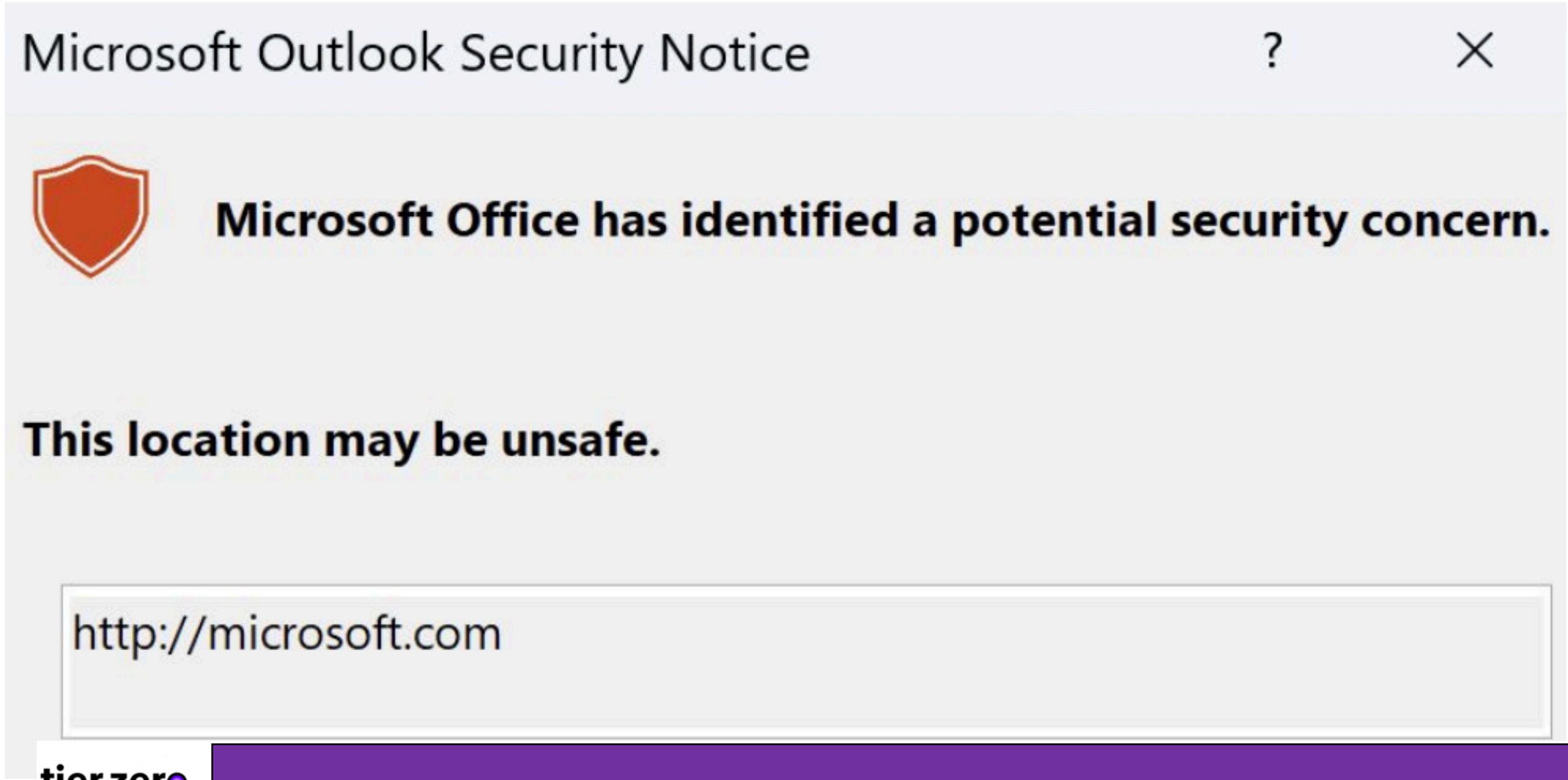
- key pairs are unique to each site, unlike passwords
- can be software based (like icloud/password managers)
- can be hardware based (like hardware tokens)
- these can remove the need for passwords as well as helping protect against phishing

Malicious documents

- Microsoft allows for various scripting languages to be run in Excel, Word etc
- great for data processing and repeatable tasks
- they also allow for a document to interact with non-document things:
  - powershell
  - cmd.exe
  - other malicious executables (bundles of code that do bad things on a computer)

Microsoft knows this is an issue

- they have the concept of Mark of the Web
- any document downloaded from an untrusted zone / the internet, contains a little flag.
- when the document opens, if MOTW is present, all those features are temporarily disabled.
- until you click some buttons.
- a lot of my security research has been bypassing these controls in MS


Microsoft Outlook Security Notice
?
Microsoft Office has identified a potential security concern.
This location may be unsafe.
http://microsoft.com

just disable them

- some users do have a legitimate business need for them
- disabling users who don't need them can decrease risk
- once again, the essential 8 is to the point here
    - restrict Microsoft Office macros

restrict administrative privileges

- this is a tricky one.
- people need to be able to do their jobs and frequently require a high level of control over their device
  - developers, sysadmins
- giving people admin rights is the ultimate 'make it go' moment
- this can backfire, but we need to try

local admin on windows is very powerful

- local admin has access to secret and credential material for all other users on the device
- on shared servers/workstations where multiple people log in, this is very dangerous

how?

- I tested an organisation (several) who had roughly 800 users, of which ~500 were in a 'local admins' users group
- made 'lateral movement' (aka moving to other computers) extremely straightforward.
- found a Domain Administrator who had logged in to a shared device
- extracted credential material and used it to authenticate: game over :-(

so we've solved it, why aren't people simply doing these things?

- "hardware MFA is expensive"
- "people will just lose them"
- "we don't have enough USB spaces on laptops"
- "if we remove people from the local admins group, everything will break"
- "we have a ten thousand seat organisation, we can't do it"

"hardware MFA is expensive"

- did you see the cost of breaches slide earlier?
- hardware tokens represent a fairly good return on investment
    - compare it to the per host cost of phishing training
- security teams are frequently seen as a cost centre
    - let's reframe security teams to a enabler of the business

"people will just lose them"

- please believe in people
- most people won't lose them
- somehow people manage to drop their phones all the time yet we still push MS authenticator pretty hard
- we have gotten used to the idea that you need a key for your car, why not your computer?
- this is why processes and service desks exist

"if we remove people from the local admins group, everything will break"

- sometimes breaking things is ok
  - says the guy who has broken things sometimes
- how you recover from this is important
- you don't have to do it all at once, you can start small

"we don't have enough USB spaces on laptops"

- "we have 2 USB, and once the keyboard, mouse and headset is in, nothing is left"
- docks exist
- bluetooth exists
    - depending on the organisation

it's hard and the process sucks sometimes

- things will break
- change is hard and it's hard to bring people along
- it starts when you can demonstrate that the new thing you want to do is:
  - safer
  - easier
  - less annoying
- but also, you have to try

you don't have to do it all at once

- start with the users who you want to protect the most
  - administrators, anyone with privileged access
- roll it out gradually
- it's ok if you need to roll it back temporarily!

what you can do right now

- ask for a hardware key from your CISO, CTO, CEO
- add it as an MFA option to the important stuff
- remove legacy MFA where hardware tokens/whatever are supported

what you can do in a month

- (if you're a security or IT person) talk to other parts of the business and users about what you're doing in the auth space
  - do it with kindness and without judgement
- if you have successful outcomes, share them with the business
- think about the edge cases
- measure change through things like:
  - hardware MFA adoption rates
  - passkey adoption rates

i believe in you

thanks!

- thanks to the OPC for having me ❤️
- thanks to my coworkers and wider information security colleagues for the enthusiastic discussions

questions?