Simplifying Security for small business
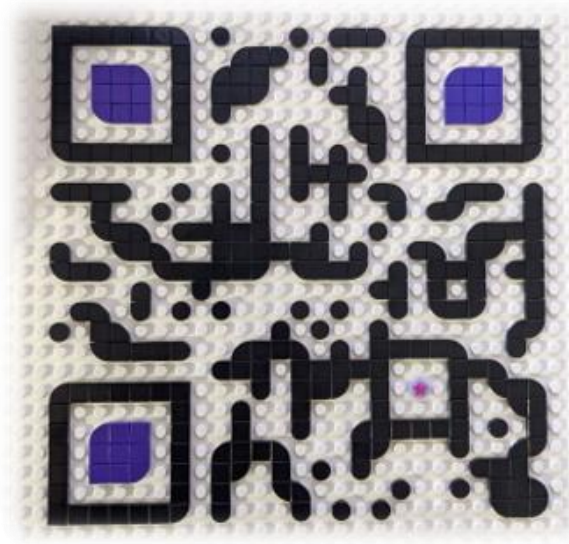
Jess Dodson

Senior Cloud Solution Architect @ Microsoft

jess.dodson@microsoft.com

Who am I?

- Senior Cloud Solution Architect @ Microsoft
- In tech for 20 years!
- Mum to a small human, an old ginger cat, chickens & some bees
- Lego collector and video game addict

- Community advocate for everyone to understand how to secure themselves digitally

So...why am I here? And what's in it for you?

Laying the foundations

Definition of Cybersecurity

Protect against Cyberattacks

Prevent Data Breaches
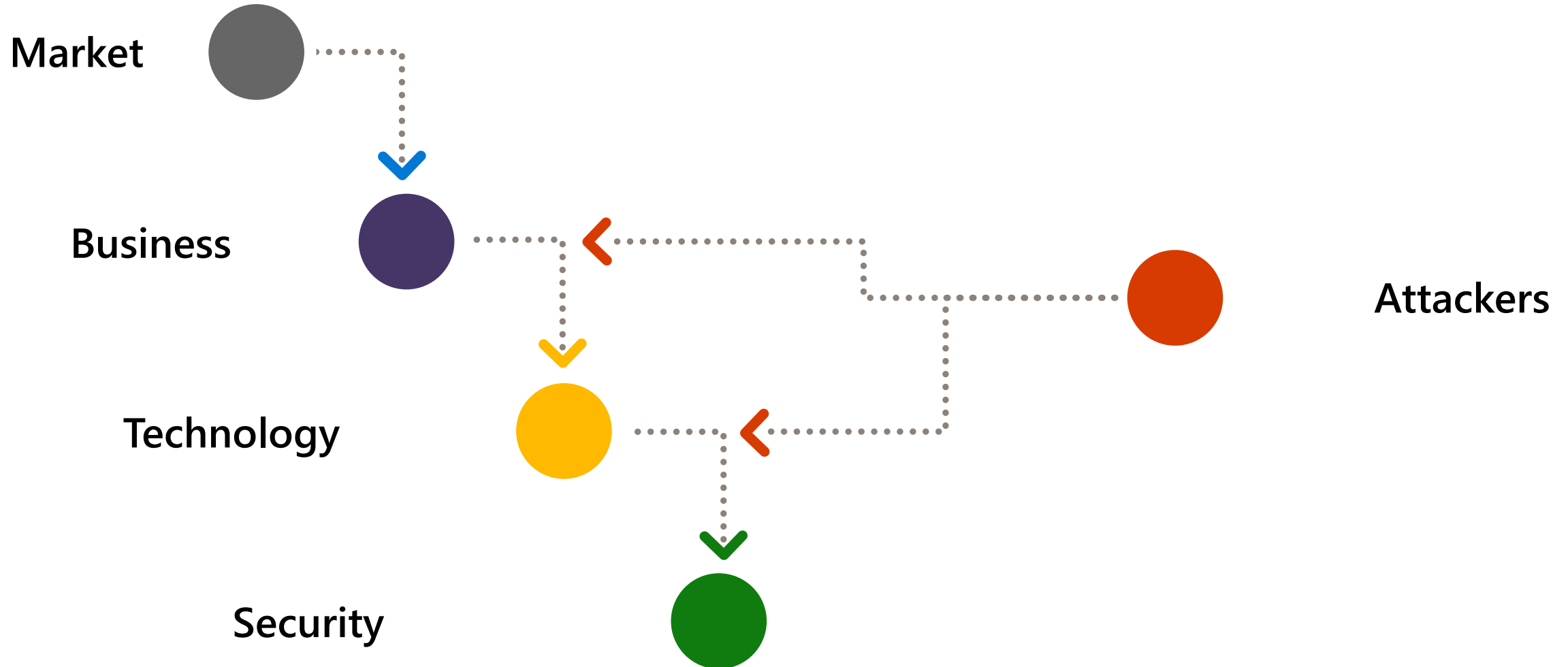
Respond to cyber security incidents

10 Laws of Cybersecurity

http://aka.ms/10Laws

Law #1	If a bad actor can persuade you to run their program on your computer, it's not solely your computer anymore.
Law #2	If a bad actor can alter the operating system on your computer, it's not your computer anymore.
Law #3	If a bad actor has unrestricted physical access to your computer, it's not your computer anymore.
Law #4	If you allow a bad actor to run active content in your website, it's not your website anymore.
Law #5	Weak passwords trump strong security.

Law #6	A computer is only as secure as the administrator is trustworthy.
Law #7	Encrypted data is only as secure as its decryption key.
Law #8	An out-of-date antimalware scanner is only marginally better than no scanner at all.
Law #9	Absolute anonymity isn't practically achievable, either online or offline.
Law #10	**Technology isn't a panacea.**

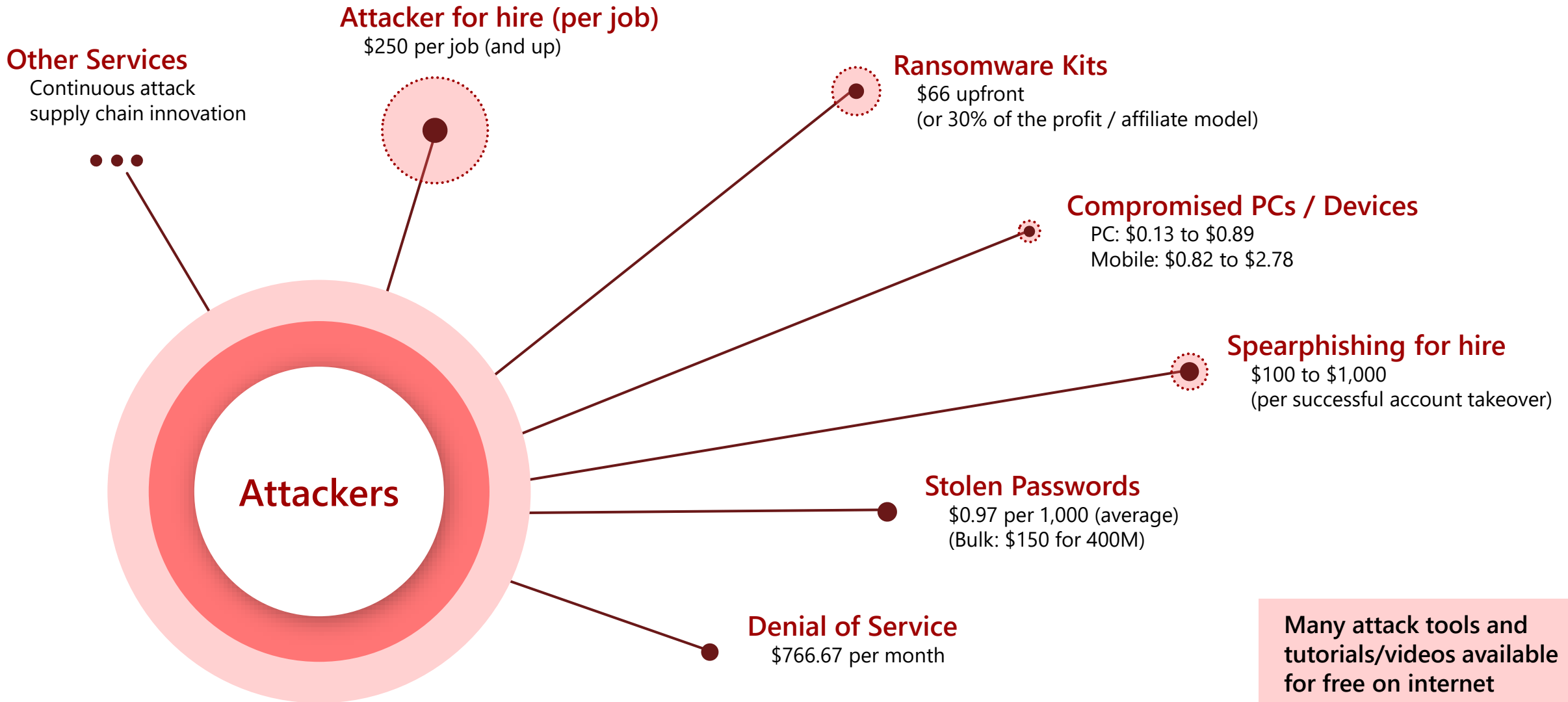# The world is transforming...rapidly

So...what do we know?

It's bad out there!
For sale in "bad neighborhoods" on the internet

Attacker for hire (per job)
$250 per job (and up)

Other Services
Continuous attack
supply chain innovation

Ransomware Kits
$66 upfront
(or 30% of the profit / affiliate model)

Compromised PCs / Devices
PC: $0.13 to $0.89
Mobile: $0.82 to $2.78

Spearphishing for hire
$100 to $1,000
(per successful account takeover)

Attackers

Stolen Passwords
$0.97 per 1,000 (average)
(Bulk: $150 for 400M)

Denial of Service
$766.67 per month

Many attack tools and tutorials/videos available for free on internet
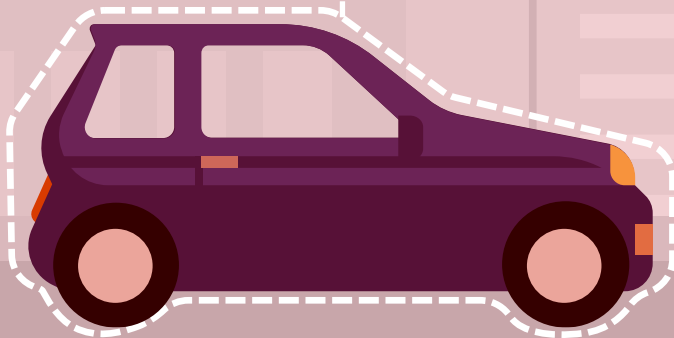
Security **is** complex... but it can be simple!

Lots of details and complexity, but just three ways to get control

Car
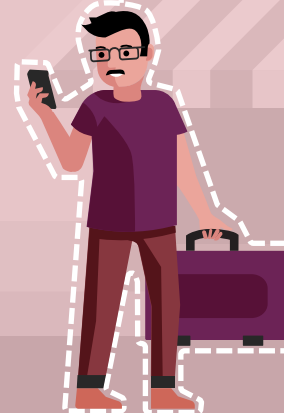*Attack technology itself (errors in software logic, configuration, etc.)*

Keys
Attack Credentials that control system(Passwords, Tokens, keys, etc)

Driver
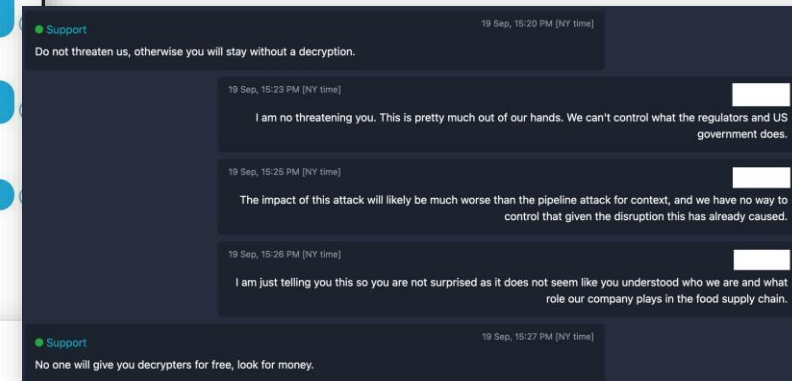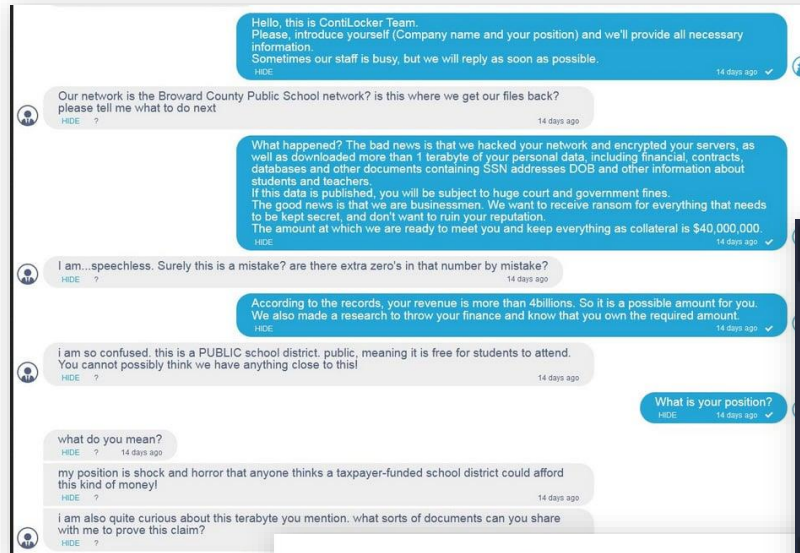*Attack People that manage/use systems (Trick, Distract or Persuade)*

Need to remember: Attackers are <u>Ruthless</u>
Criminal gangs can and will disrupt/halt all business operations

They will target
any organization

- Often demand ridiculous payment
- Don't care who it hurts
- They can and <u>will</u> retaliate

→ **Ransomware overview and guidance**
aka.ms/humanoperated

The 4 primary threats to all organizations

Phishing

Deceptive emails, websites, and text messages to steal confidential information.

Identity and Devices

Protecting devices and updating software is vital to avoid identity theft.

Ransomware

Some scams will ask you to pay to "fix" a nonexistent problem or demand a ransom for your data.
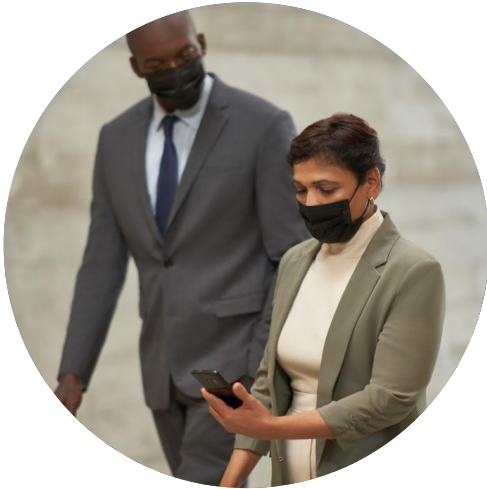

Passwords

Going passwordless or using multi factor authentication is crucial for online safety.

...so, what more do we know & what can we DO?

Phishing & Ransomware

Phishing

Deceptive emails, websites, and text messages to steal confidential information.

Identity and Devices

Protecting devices and updating software is vital to avoid identity theft.
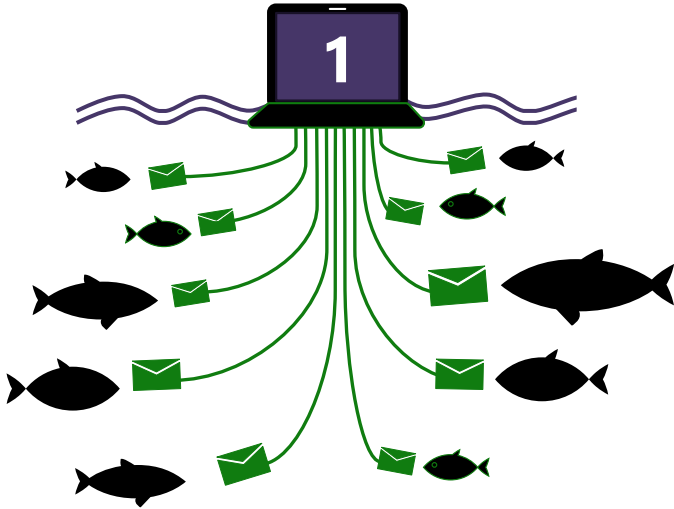
Ransomware

Some scams will ask you to pay to "fix" a nonexistent problem or demand a ransom for your data.
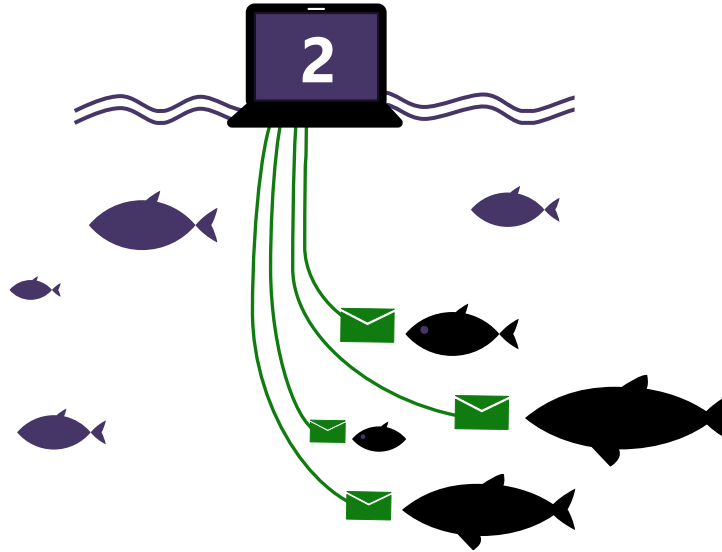
Passwords

Going passwordless or using multi factor authentication is crucial for online safety.
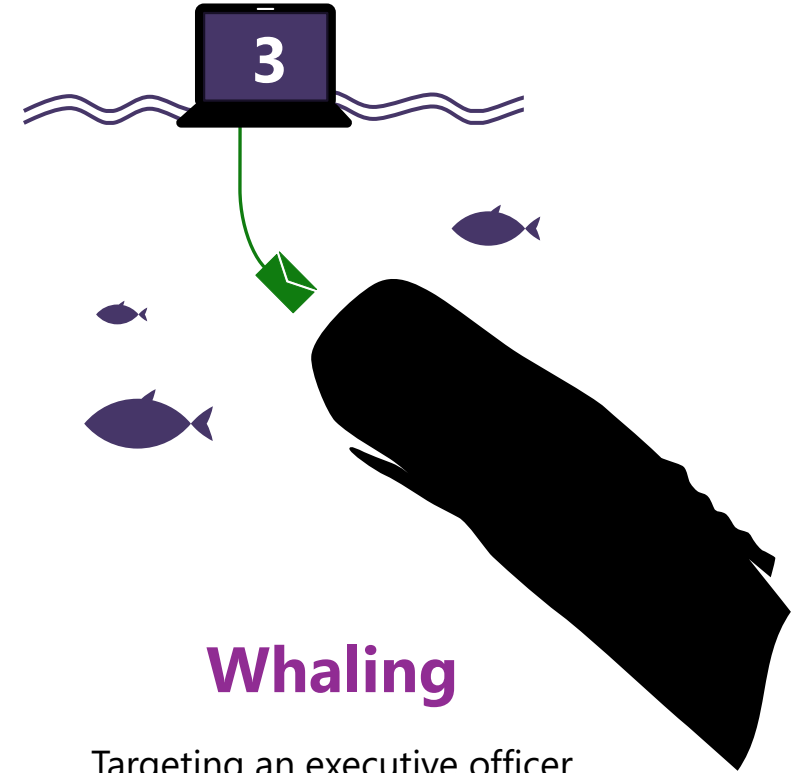
Phishing types

Phishing

Targeting an entire organization with a generic campaign

Spear phishing

Targeting a specific group within an organization with a custom campaign

Whaling

Targeting an executive officer within an organization with a personalized campaign

Ransomware – how does it happen?

1 **Stolen passwords and unprotected identities**

2 **Missing or disabled security products**

3 **Misconfigured or abused applications**

4 **Slow patching**

What to look for?

security sms spoof outlook connection response risks

government app authentication breach

fake reset unfamiliar liability accounts copyright statement unique

hacked logins verification two-factor payment protect

compromised send recommends review cyber attacker spyware

unauthorised help account case registered phone scam recovery web

email sign-in address services business invoice financial

guidance password update passwords 20

identity user microsoft crime information social

contact access threat login sensitive standard

immediately may

support organisations available damage devices

incident online ransomware free

locked document ransom gmail

safeguard mfa

protection prevent activity form reputation

Phishing examples

Dear Customer ,

After completing the annual calculation of your personal fiscal dues, we are delighted to inform you that you will receive a tax refund of 638.64 AUD

We sincerely apologize for this inconvenience and would like to inform you that our teams are continuously working on improving our working processes to avoid similar issues in the future. To receive your tax refund, please complete the following form click here:

Complete Your Information

https://wordpress-941091-3271416.cloudwaysapps.com/wp-admin/AUJMQXSSBVMOBYQBSSWL/

TAX ID: AU*******

Status: Missing information

You received this e-mail because you are registered with myGov

---

Your package N°9L26854905403 will not be delivered today.

AP   Australia Post® <morfos@aireconseil.fr>
To
Fri 10/02

ⓘ If there are problems with how this message is displayed, click here to view it in a web browser.

Australia Post   VIEW ONLINE

Hello

Your package N°9L26854905403 will not be delivered today.

Your package cannot be delivered today due to an exceptional situation beyond our control or because access to the delivery address is impossible.
The information at our disposal did not allow us to ensure delivery.
To organize the second presentation, Please click here

We apologize for any inconvenience this unexpected event may cause.

Archie Alexander <clariceclaude810@gmail.com>
07:58 (1 hour ago) ☆ ↩ ⋮
to me ▾

Why is this message in spam? It is similar to messages that were identified as spam in the past.

Report as not spam
ⓘ

Multi-Layered Theft Protection System

Confirmation Date – 07-11-2024

Receipt# : 1178392500399

Receipt to > jess@girl-germs.com

Thank You for Entrusting Us with Your Online Security

It has been an amazing year since you became a part of our Security Services Community, and we are incredibly thankful for the chance to serve you. Today, we are celebrating a major milestone. We hope that the McAfee product, which you bought using PayPal, has given you more than what you expected in terms of top-notch security and total tranquility.

McAfee

Thanks for Shopping with Us!

Product Information

Product :	McAfee® Web Advisor
Term :	1 Year
Pay via :	Card/ Auto-Debit/ Online
Qty:	1
Total Price :	**$599.28**

PayPal

Please Note :-

If you wish to make any changes or cancel your purchase for a full refund, simply reach out to our experts at:

+61 242 048 113

Support scams

Spot the scam signs

Authority

Is the message claiming to be from someone official?

Like your bank, a government department, a utility company, your doctor or a solicitor. Criminals pretend to be important people or organisations to trick you into doing what they want.

Emotion

Does the message make you panic, fearful, hopeful or curious?

Scammers use threatening language, make false claims of support, or tease you into wanting to find out more.

Current events

Are you expecting to see a message like this?

To make their scam seem more real, criminals can exploit current news stories and events. For example, some scammers pretend to be from the tax office at tax time to make their scam seem more relevant.

Urgency

Are you told you have a limited time to respond?

For example, 'within 24 hours' or 'immediately'. Criminals often threaten you with fines or other negative consequences.

Scarcity

Is the message offering something that seems too good to be true?

Like concert tickets, money or a cure for medical conditions? Fear of missing out on a good deal or opportunity can make you respond quickly.
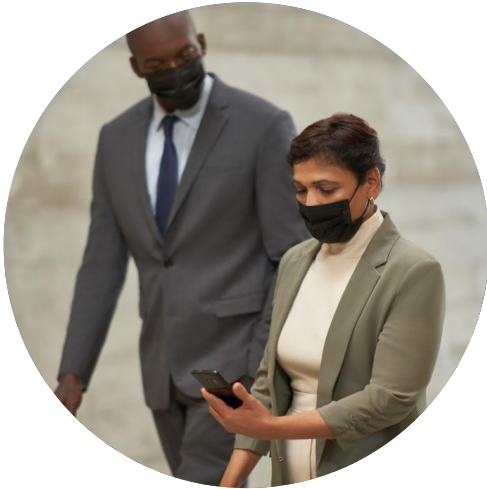
3 – 2 – 1: BACKUP!

https://www.pcmag.com/picks/the-best-cloud-backup-services-for-business

Identities, devices & passwords

Phishing

Deceptive emails, websites, and text messages to steal confidential information.

Identity and Devices

Protecting devices and updating software is vital to avoid identity theft.
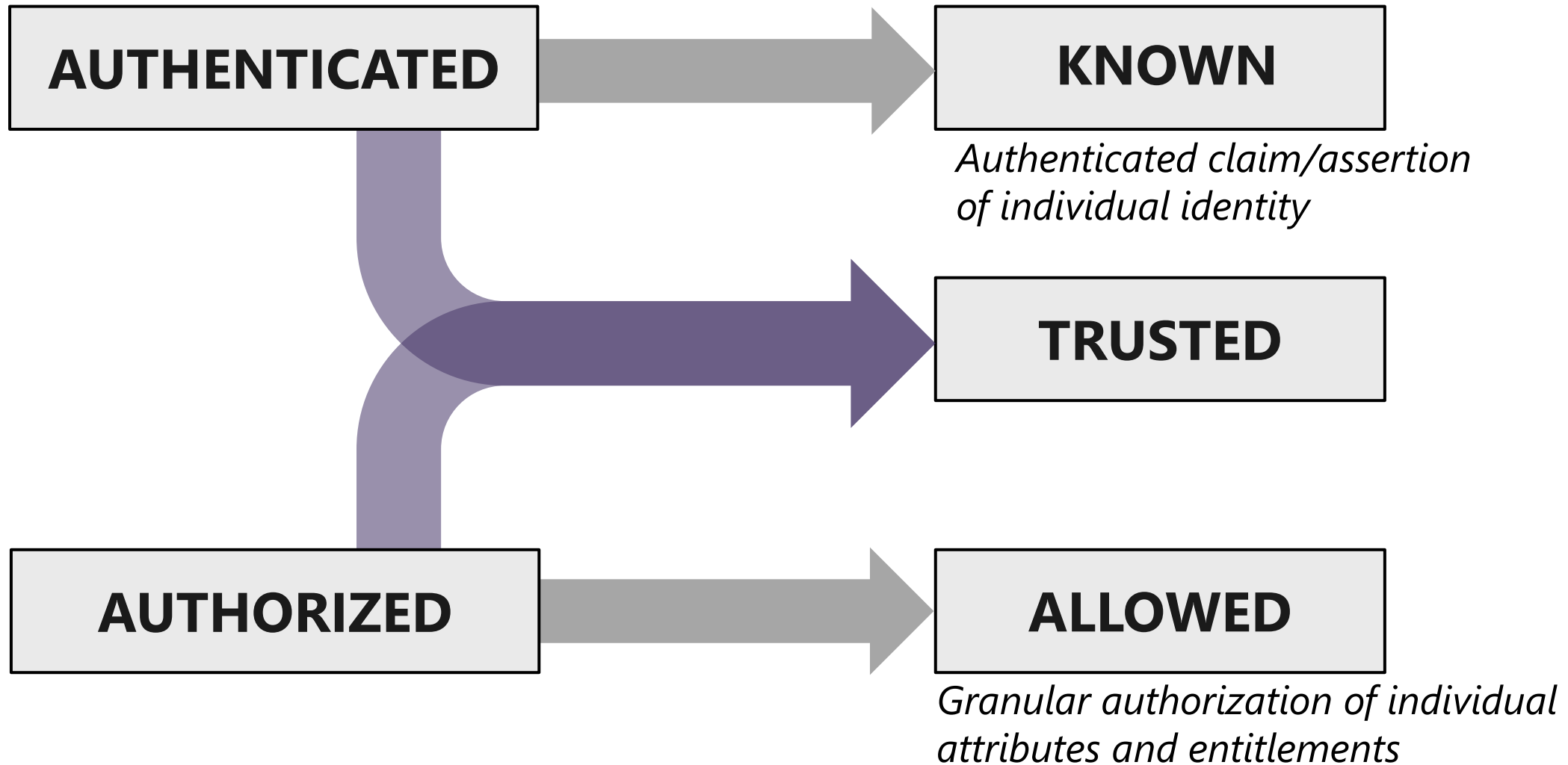
Ransomware

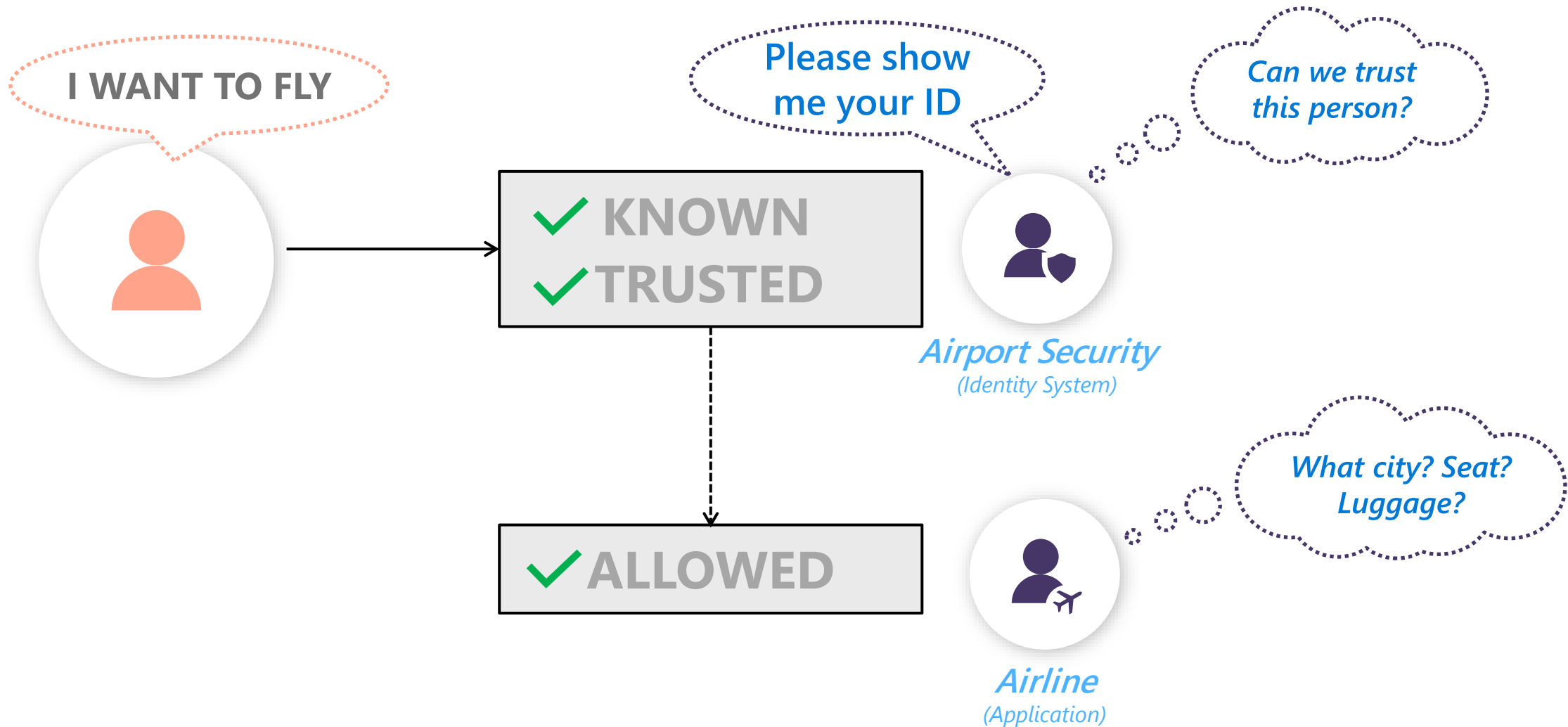Some scams will ask you to pay to "fix" a nonexistent problem or demand a ransom for your data.

Passwords

Using multi factor authentication or going passwordless is crucial for online safety.

Evolution of Authentication and Authorization

AUTHENTICATED → **KNOWN**

Authenticated claim/assertion of individual identity

TRUSTED

AUTHORIZED → **ALLOWED**

Granular authorization of individual attributes and entitlements

Air travel analogy

So, what makes a good password?

Best practices for accounts & passwords

What is?

One of the most important ways to ensure that your online accounts are safe and secure is to protect your passwords. Follow this advice to help keep your accounts out of the wrong hands.

Here are 4 easy rules to keep your email, accounts, and devices safer and avoid identity theft:

1 Create strong passwords (better: passphrases!)
- o At least 12 characters long but 14 or more is better.
- o Combination of uppercase and lowercase letters, numbers, and symbols.
- o Significantly different from your previous passwords.
- o ^ DO NOT reuse passwords!

2 Secure your Passwords.
- o Don't share a password with anyone.
- o Use a password manager for multiple passwords.
- o Change passwords immediately on accounts you suspect may have been compromised.

3 Don't be tricked into revealing your passwords
- o Be wary of anyone who is requesting sensitive info from you, even if it is an interaction you trust.
- o Never share passwords answering emails or phone calls.
- o Always access websites using trusted links.

4 Enable MFA/2FA whenever available
- o They can't steal your password if you don't use one!
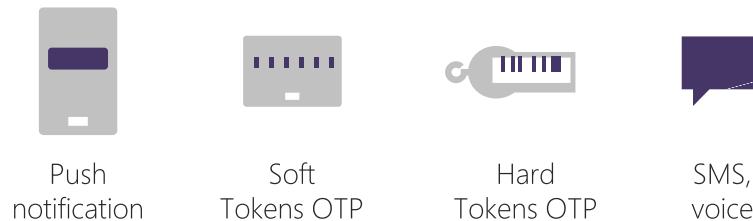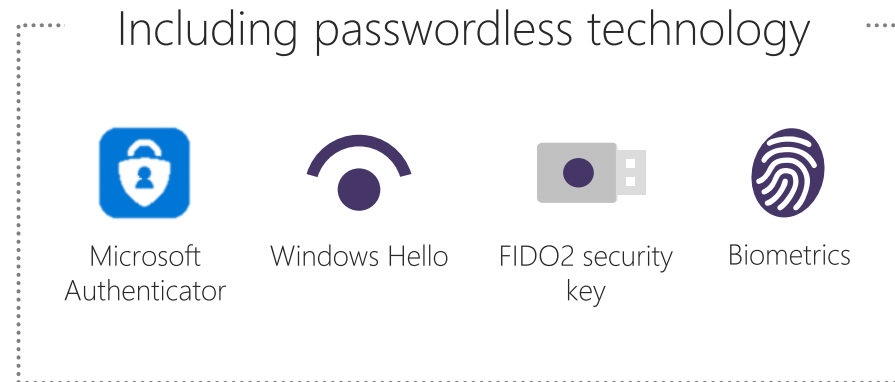- o Use authenticator apps

Managing passwords

Multi-factor authenticator (MFA or 2FA)

Multi-factor authentication (MFA) requires you to prove your identity in __2 or more ways__ before you can access your device or account.
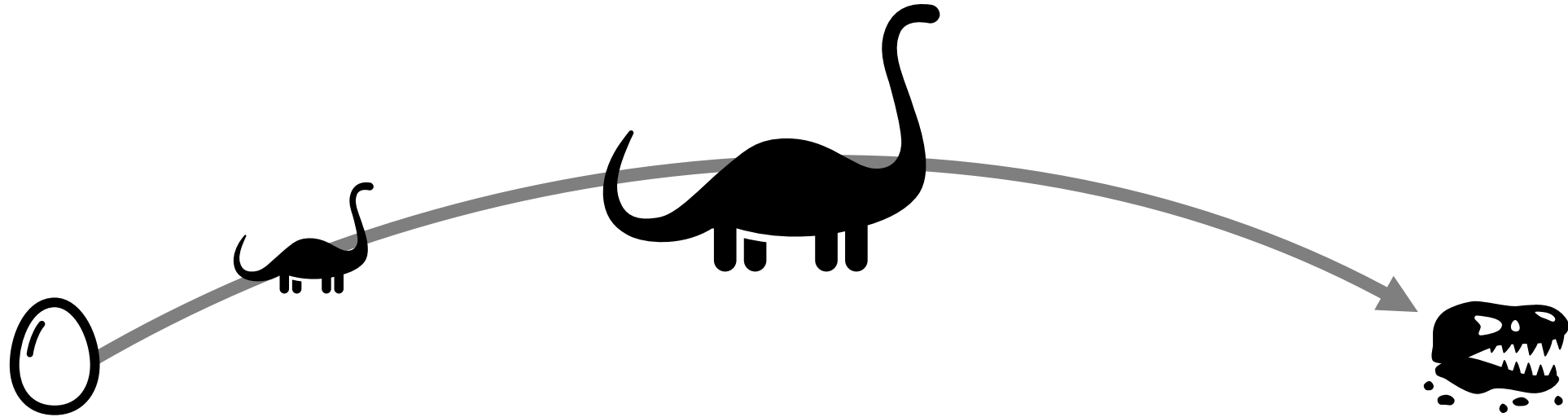
There are a huge range of multi-factor technologies available!

Including passwordless technology

Microsoft Authenticator

Windows Hello

FIDO2 security key

Biometrics

Push notification

Soft Tokens OTP
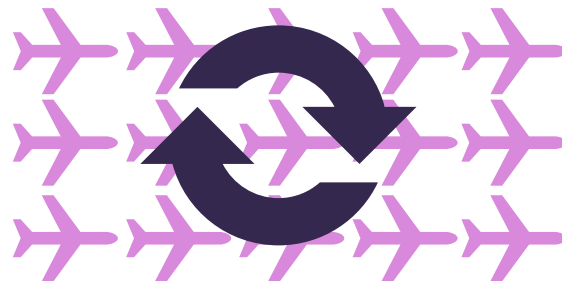
Hard Tokens OTP

SMS, voice

Multi-factor authentication prevents 99.9% of identity attacks

All things grow, age, & die – including IT systems!

A healthy fleet of business assets requires:

1. **Maintaining assets** to avoid downtime/disruption
2. **Retiring and replacing assets** when useful life ends

Best practices for your identities & devices

What is? Protecting devices and identity is important for keeping your emails, accounts, and devices safer and avoiding identity theft. Learn ways for never having to replace all identification, credit cards, and official documents after having identities stolen by cyber criminals.

Here are 8 easy rules to keep your identities and devices safer:

1 Share personal information in real time only, preferably in person or by phone to trusted individuals or organisations only.

2 Be skeptical of messages with links, especially those asking for personal information.

3 Be on guard against messages with attached files.

4 Use a password manager or consider going passwordless.

5 **Enable the lock feature on all your mobile devices.**

6 **Install software updates immediately and ensure all the apps on your device are legitimate.**

7 **Use the latest Windows/iOS version.**

8 **Keep your browser updated and enable Pop-Up Blocker.**

Take-aways

Top 5 security take-aways

1 Use strong passwords and make **all** passwords unique

2 Turn on multifactor authentication on **all** your accounts

3 Keep **all** your devices and software updated

4 Backup **all** important data

5 Learn to **recognize** and report phishing (scamwatch.gov.au)

ID Care | www.idcare.org.au

- IDCare: IDCARE for Small Business Cyber Health Check
- Fact Sheets: IDCARE Fact Sheets

iD care

SUPPORT SERVICES ⌄   LEARNING CENTRE ⌄   ABOUT IDCARE ⌄   CONTACT US

DOES YOUR SMALL BUSINESS NEED ASSISTANCE?

Our Services Are Available And Free

If you are experiencing an incident or aren't sure, click on the **Get Help button** to have one of our incident responders assess what's going on and call you in a time window that you nominate, or call us on **1800 595 170** Monday to Friday 8am-6pm AEST.

Get Help Now

Government Resources

- Australian Cyber Security Centre: [Small Business Cyber Security](#)

- Business.gov.au: [Cyber security and your business](#)

- Queensland: [Cyber Security Support Program | QLD Gov](#)

- New South Wales: [Cyber security awareness | NSW Gov](#)

- Canberra: [Protect your business | ACT Gov](#)

- Victoria: [Manage cybersecurity in your business | Vic Gov](#)

- Tasmania: [Cyber security | TAS Gov](#)

- South Australia: [Cyber Uplift for small business | SA Gov](#)

- Northern Territory: [Cyber Security | NT Gov](#)

- Western Australia: [Cyber security | WA Gov](#)

Cloud Provider & Tech SMB Security resources

Microsoft | Cybersecurity for small and medium business

Amazon | Cloud Data Security Solutions for SMBs

Google | Security checklist for small businesses (1-100 users)

Microsoft Blog | 7 cybersecurity trends for small and medium businesses | Microsoft Security Blog

Have I Been Pwned | haveibeenpwned.com

CyberWardens | cyberwardens.com.au

Thank you!

Any questions?

Jess Dodson
jess.dodson@microsoft.com
https://www.linkedin.com/in/jrdodson/