ARTEVOLVE WEBINAR SERIES

Cybersecurity Masterclass: What Every Art Organization Needs To Know

With Mackenzie Garrity,
CCO of Articheck, and
Federico Feliziani, CTO of Articheck

Presented by articheck

Today's ArtEvolve

CYBERSECURITY MASTERCLASS

- Art world cybersecurity concerns
- Top 10 cybersecurity terms
- 5 Actions to take right now

ART WORLD CONSEQUENCES

- THEFT
  - location
  - value

- Reputation damage
  - client data
  - artist data

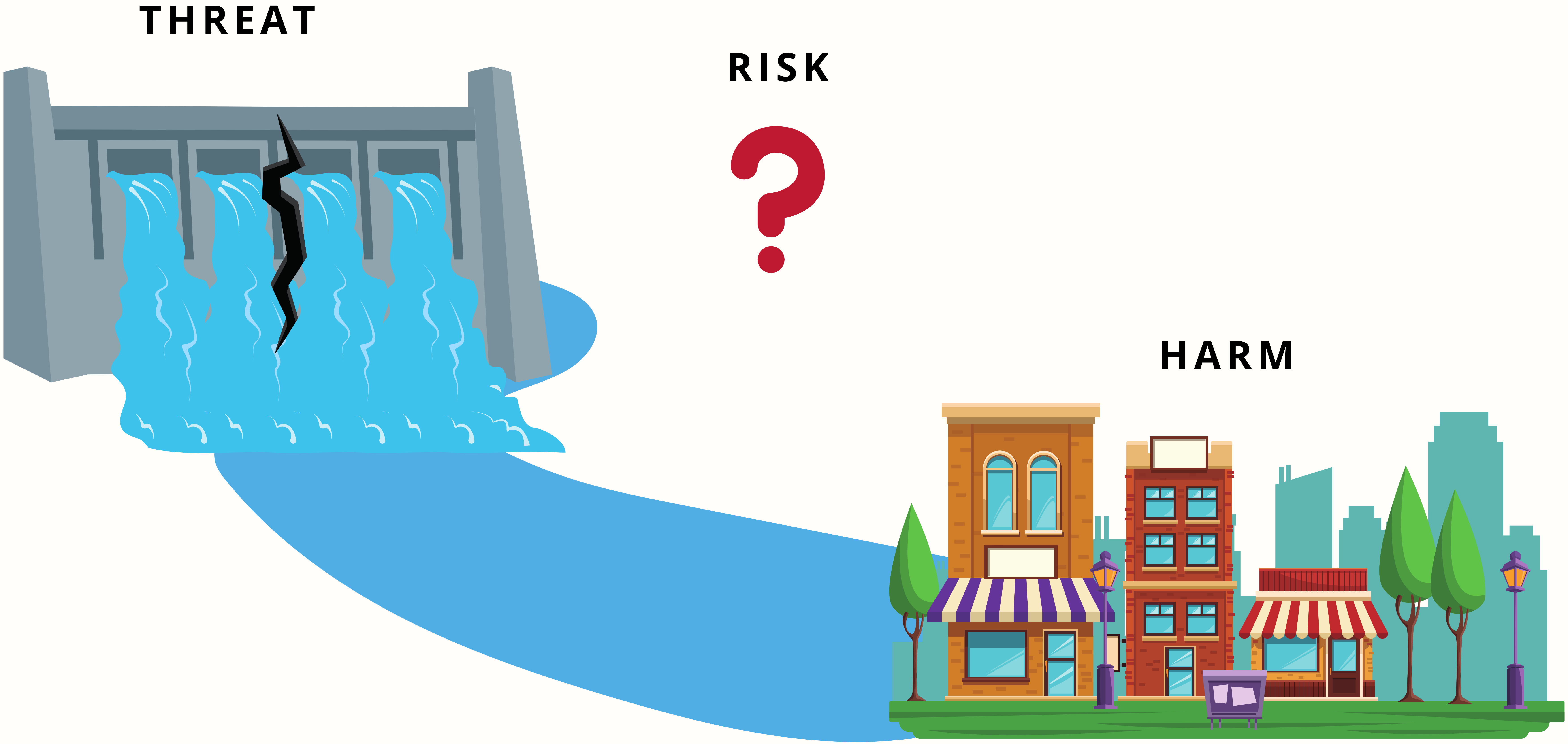
- Monetary loss
  - institution funds
  - client money

- Fraud
  - taking
  - adding info

- Loss of control
  - can't work!

TOP 10 TERMS

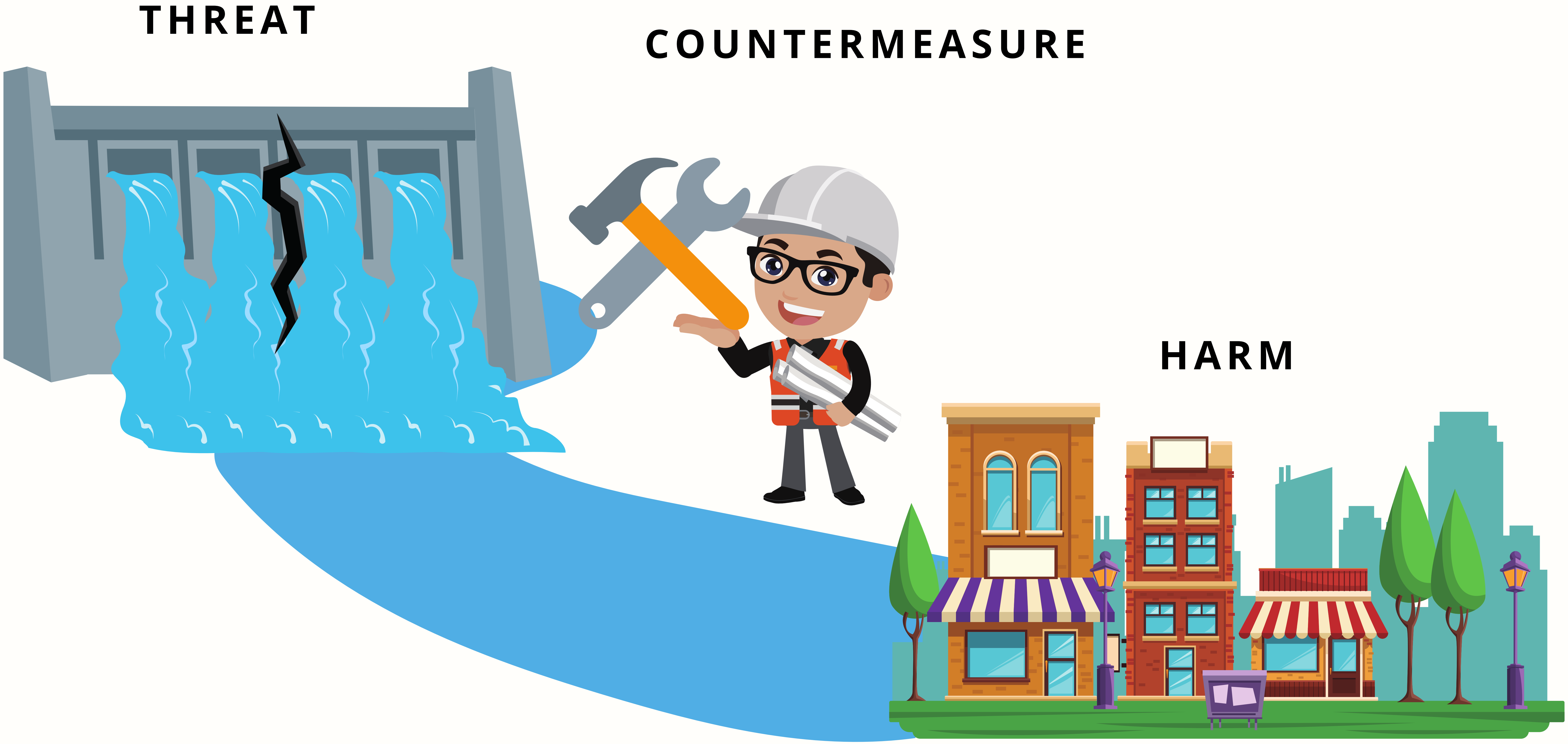
1. Risk
2. Harm
3. Threat
4. Countermeasure/Mitigation
5. OWASP Top 10
6. Authorisation
7. Authentication
8. Encryption
9. 2FA
10. Cloud



THREAT

RISK

HARM



THREAT

COUNTERMEASURE

HARM

OWASP Top 10

The Ten Most Critical Web Application Security Risks

Open Web Application Security Project® is a nonprofit foundation that works to improve the security of software.

The OWASP Top 10 is a standard awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to web applications.

use to inform internal strategy

AUTHENTICATION VS AUTHORISATION

Authentication

Verifies the identity of a user or service

Authorisation

Determines their access rights

Encryption:

A way of translating data from plaintext (unencrypted) to ciphertext (encrypted).

Users can access encrypted data with a key.

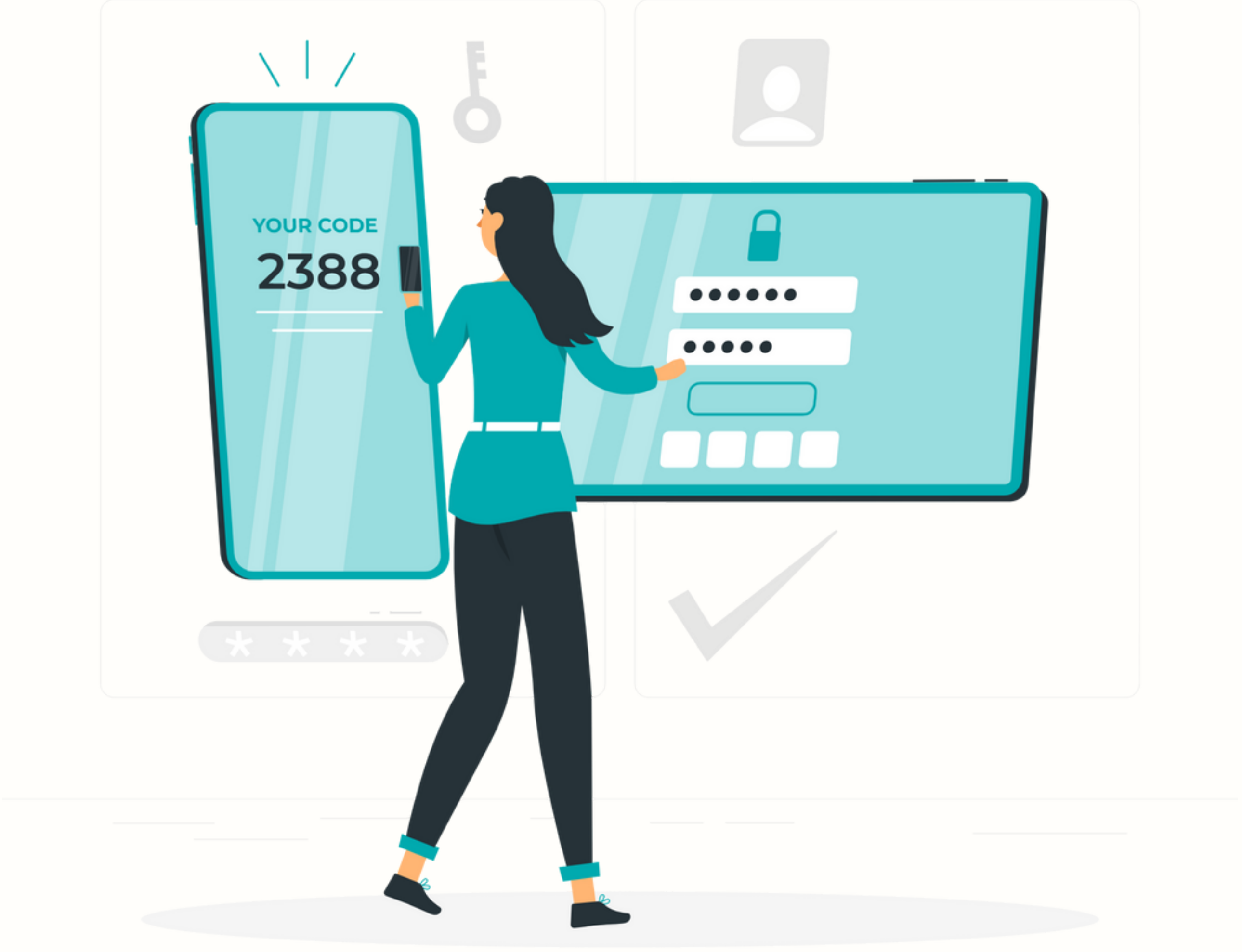
2FA - Two Factor Authentication

Strengthens access security by requiring two methods (authentication factors) to verify identity.

something you know
(username & password)

+

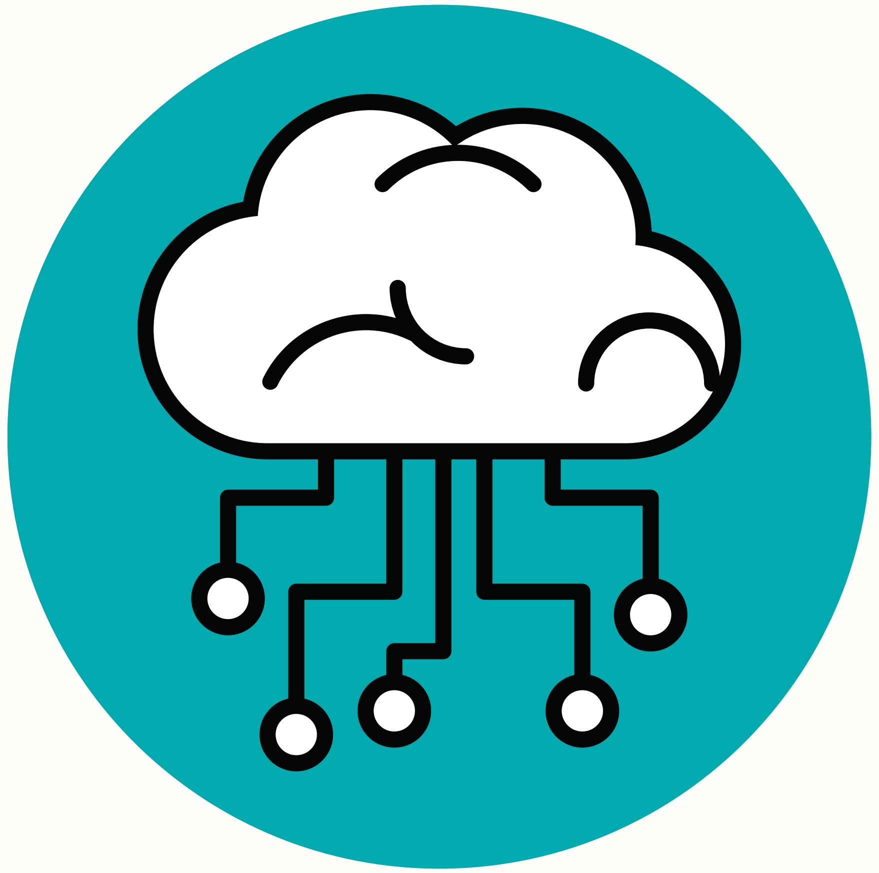
something you have
(device/account)



Cloud

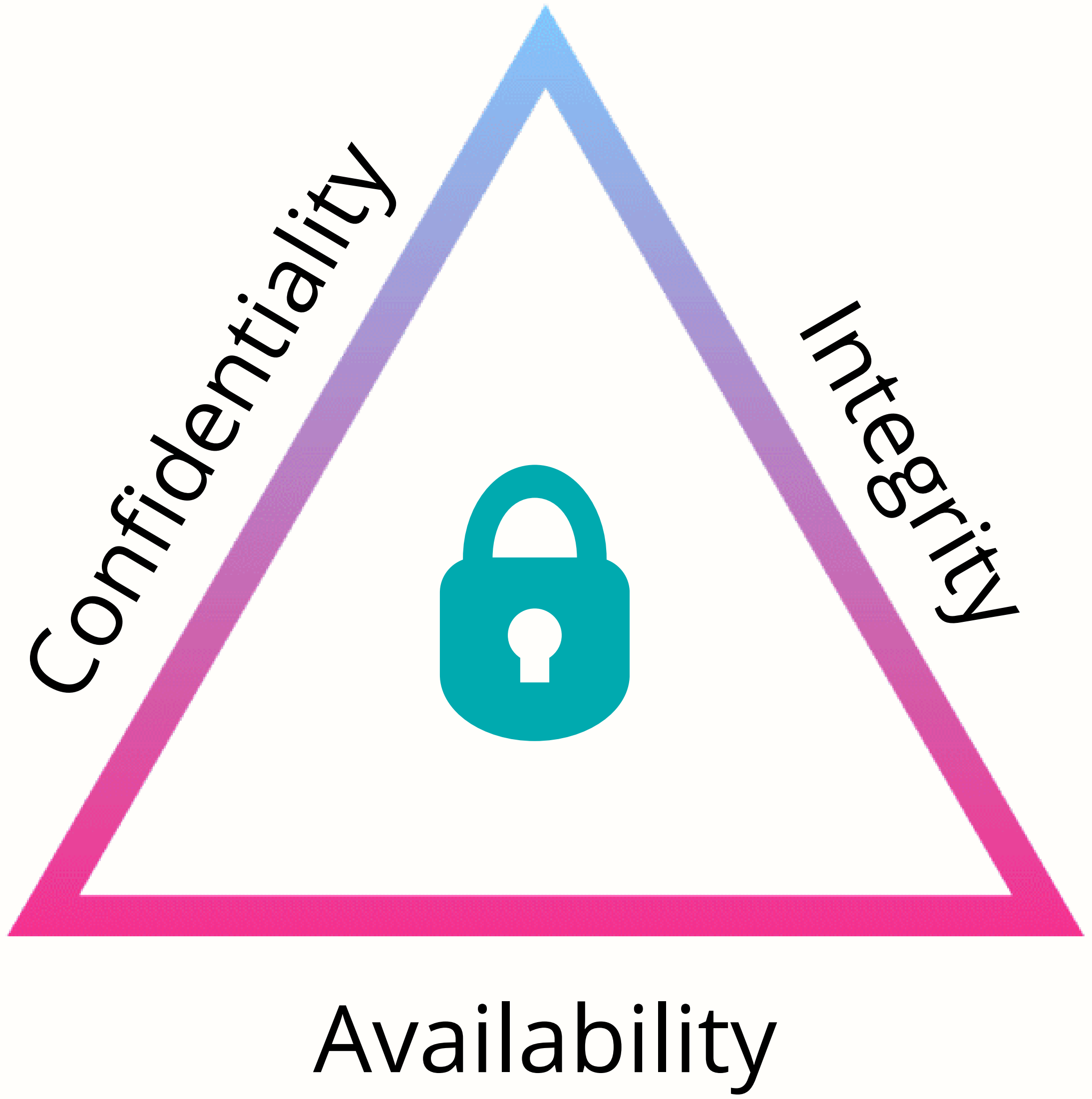
Cloud computing is access to computer system resources via the internet without direct physical management by the user.

Often distributed across multiple locations.



5 THINGS YOU CAN DO RIGHT NOW

1.Send Sensitive Data Securely



- Email is one of the most easily hacked forms of communication

- Emails can be forwarded on to unknown recipients

- Content can be changed/manipulated once sent, e.g. PDFs

- Information can be taken out of context

How To Send Sensitive Data Securely

Sometimes you have to let go of perceived control to improve security

AUTHENTICATION & ACCESS USING THE CLOUD

2.Use 2FA - Two Factor Authentication

- Usernames + passwords can easily be hacked
- Easily memorizable passwords are unsecure e.g. Password1
- Reusing passwords across accounts/websites compromises security of all

2.Use 2FA - Two Factor Authentication

- Mobile
- Email
- Apps
- Hardware Token
- SMS ⚠
- Biometric

3.Keeping Software Updated

- Hackers are always working and coming up with new ways to attack
- New software developments and improvements can prevent attacks in new ways
- Usability of software – app vulnerabilities are a way in for hackers

4.Hardware Best Practices

- Password protection & screen timeouts
- Consider replacing devices – OS of old hardware can't be updated
- Regular backups – physical hardware can be lost
- Decommissioned devices contain sensitive info

5.Encourage Employee Education

- Employees are often the first to see/interact with threats = first line of defence

- Majority of breaches caused by human error

- Understanding threats encourages responsibility/action

5.Encourage Employee Education

- Training + teaching to spot suspicious activity e.g. phishing emails
- Reinforce best practices e.g. enforce password changes, lowest permission level when sharing data.
- Write a company security policy, start with 1 page, use this presentation as a reference!

artevolve

webinar series

Presented by articheck