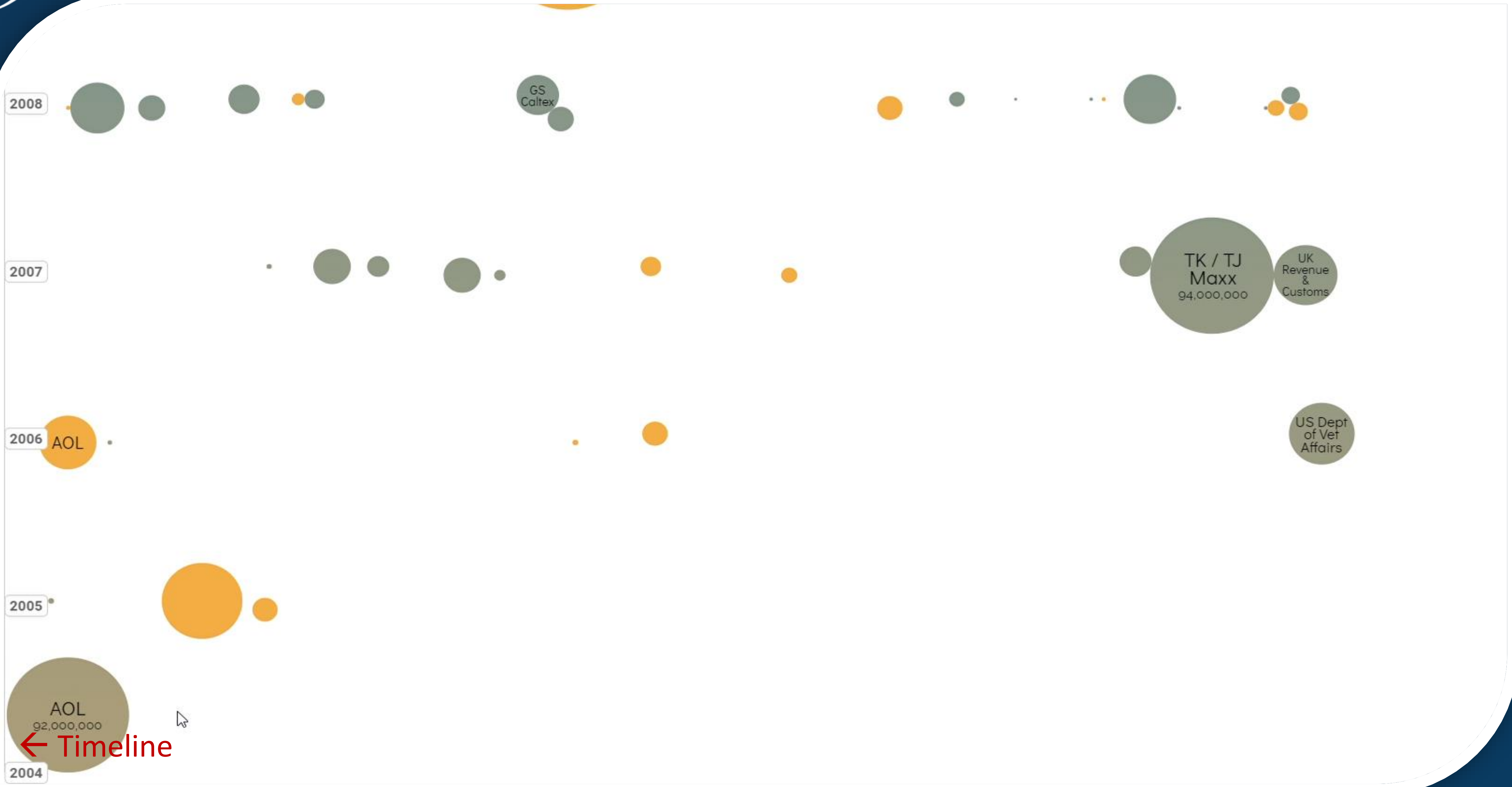
# Welcome! The Event will start at 13:04



← Timeline

MBA ASSOCIATION OF IRELAND

Strategies to help you protect your most valuable assets
10/06/2021

# "Cyber Security & Internet Fraud"

intuity

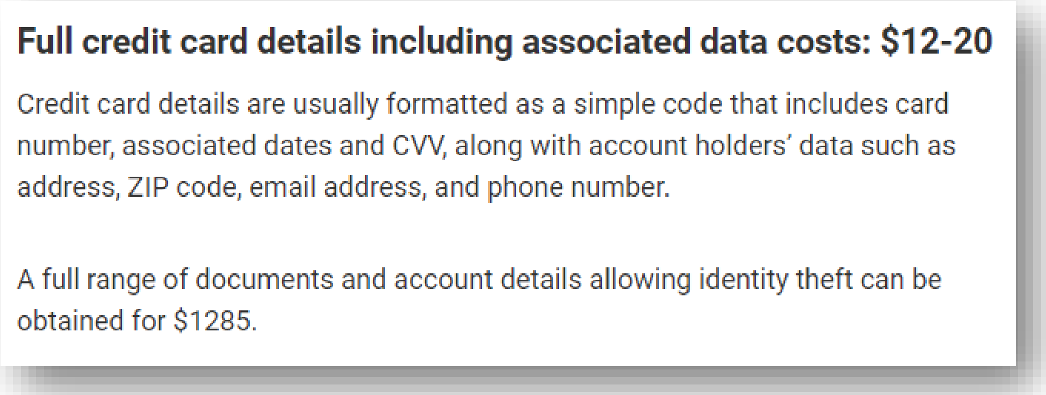
# But how much is it worth?

*How much does my Credit Card information cost on the Dark Web?*

*Please enter your answer in the Meeting Chat…*

# But how much is it worth?

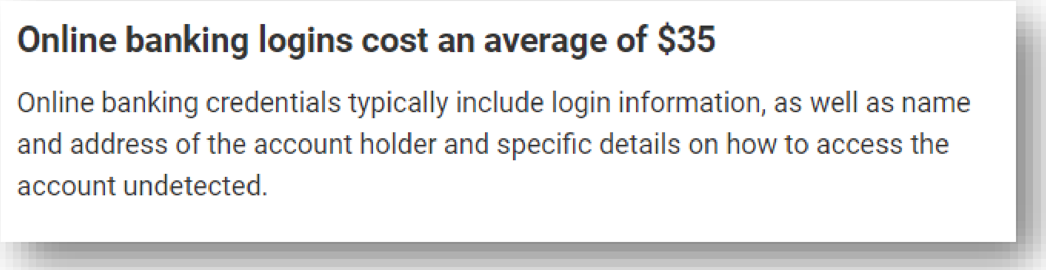
*$12 - 20*



### Full credit card details including associated data costs: $12-20

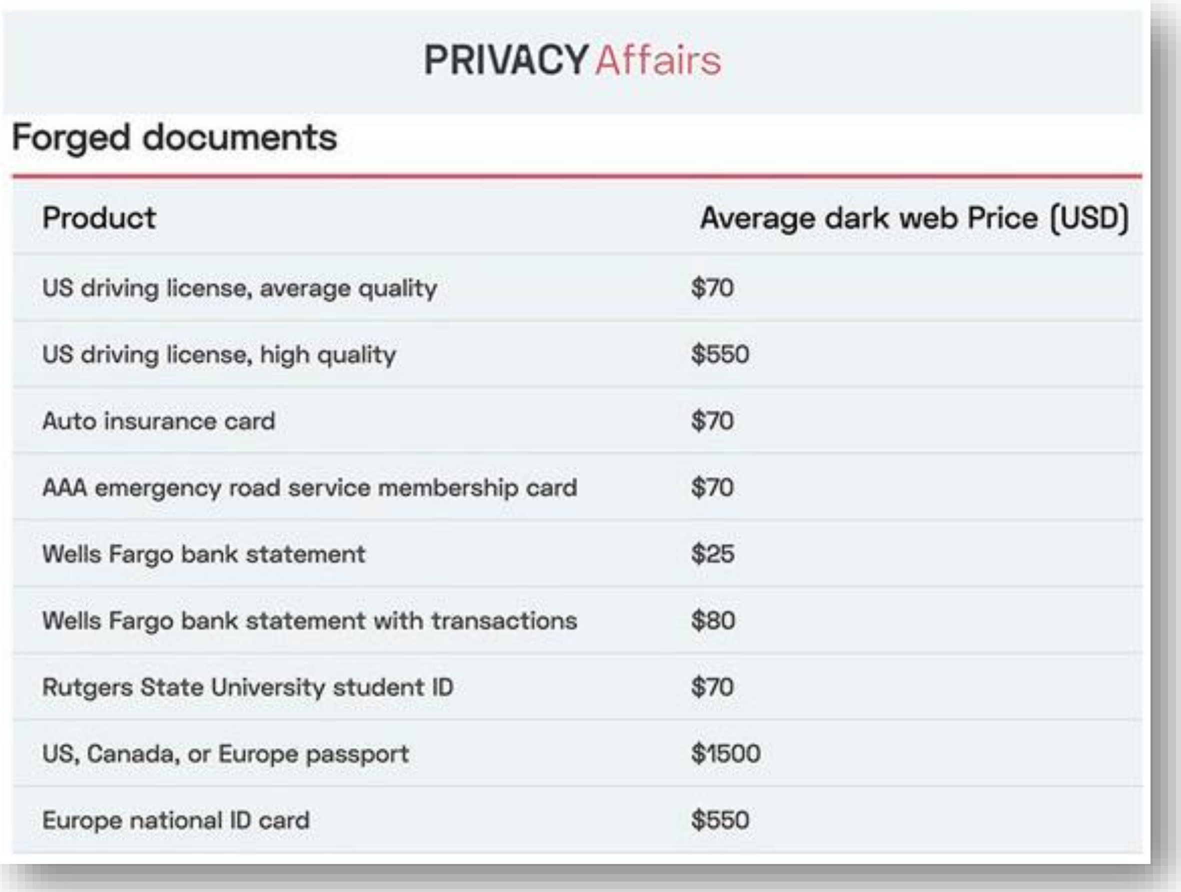
Credit card details are usually formatted as a simple code that includes card number, associated dates and CVV, along with account holders' data such as address, ZIP code, email address, and phone number.

A full range of documents and account details allowing identity theft can be obtained for $1285.



### Online banking logins cost an average of $35

Online banking credentials typically include login information, as well as name and address of the account holder and specific details on how to access the account undetected.



PRIVACY Affairs

### Forged documents

| Product | Average dark web Price (USD) |
|---|---|
| US driving license, average quality | $70 |
| US driving license, high quality | $550 |
| Auto insurance card | $70 |
| AAA emergency road service membership card | $70 |
| Wells Fargo bank statement | $25 |
| Wells Fargo bank statement with transactions | $80 |
| Rutgers State University student ID | $70 |
| US, Canada, or Europe passport | $1500 |
| Europe national ID card | $550 |

# This is how fast a password leaked on the web will be tested out by hackers

Cybersecurity researchers planted phoney passwords on the web. They found that attackers were extremely quick to test if usernames and passwords worked.

By Danny Palmer | June 8, 2021 -- 15:32 GMT (16:32 BST) | Topic: Security

ZDNet
Business Email Compromise phishing attacks could be the most costly threat facing your organizations
WATCH NOW
ZDNet security update

Half of accounts compromised in phishing attacks are manually accessed within 12 hours of the username and password being leaked, as cyber criminals look to exploit stolen credentials as quickly as possible.

MORE FROM DANNY PALMER

Security

**This new ransomware group claims to have breached over 30 organisations so far**

Productivity

**A massive outage just took large sections of the internet offline**

Security

**Diversity in cybersecurity: How being inclusive can help improve everyone's defenses against attacks**

Security

**This phishing email is pushing password-stealing malware to Windows PCs**

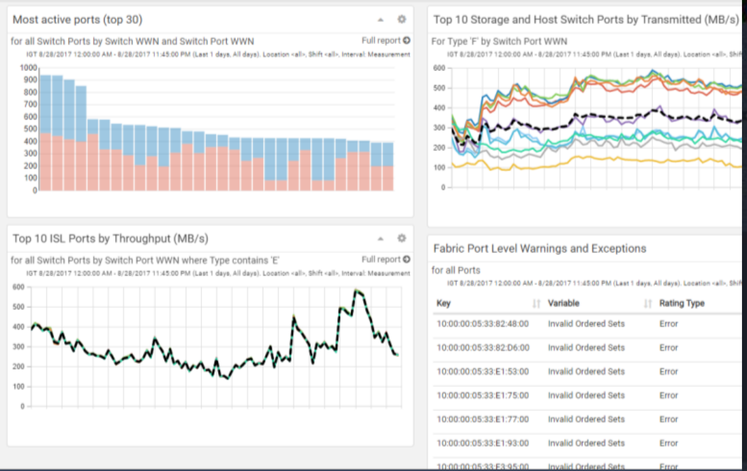
# Our Purpose @ Intuity

*We believe that every business should have the opportunity to grow, improve, thrive and prosper in a secure technological environment.*

*For us, it’s about protecting companies and people’s livelihoods.*

Adam Banks, Chief Technology & Information Officer, Maersk
Keynote Presentation
Case Study: Lessons Learned from the NotPetya Cyber-Attack
KEYNOTE
KEYNOTESTAGE
Microsoft

G120
Securing the Data Journey
FORTINET
Securing The Data Journey
With the Fortinet Security Fabric providing a Broad, Integrated and Automated architecture across the entire network



Most active ports (top 30)

for all Switch Ports by Switch WWN and Switch Port WWN — Full report

IGT 8/28/2017 12:00:00 AM - 8/28/2017 11:45:00 PM (Last 1 days, All days). Location <all>, Shift <all>, Interval: Measurement

Top 10 Storage and Host Switch Ports by Transmitted (MB/s)

For Type 'F' by Switch Port WWN

IGT 8/28/2017 12:00:00 AM - 8/28/2017 11:45:00 PM (Last 1 days, All days). Location <all>, Shif

Top 10 ISL Ports by Throughput (MB/s)

for all Switch Ports by Switch Port WWN where Type contains 'E' — Full report

IGT 8/28/2017 12:00:00 AM - 8/28/2017 11:45:00 PM (Last 1 days, All days). Location <all>, Shift <all>, Interval: Measurement

Fabric Port Level Warnings and Exceptions

for all Ports

IGT 8/28/2017 12:00:00 AM - 8/28/2017 11:45:00 PM (Last 1 days, All days). Location <all>, Shif

| Key | Variable | Rating Type |
|---|---|---|
| 10:00:00:05:33:82:48:00 | Invalid Ordered Sets | Error |
| 10:00:00:05:33:82:D6:00 | Invalid Ordered Sets | Error |
| 10:00:00:05:33:E1:53:00 | Invalid Ordered Sets | Error |
| 10:00:00:05:33:E1:75:00 | Invalid Ordered Sets | Error |
| 10:00:00:05:33:E1:77:00 | Invalid Ordered Sets | Error |
| 10:00:00:05:33:E1:93:00 | Invalid Ordered Sets | Error |
| 10:00:00:05:33:E3:95:00 | Invalid Ordered Sets | Error |

Case Management Overview

# Getting to know the Threats

- Security & Compliance Team
- Emerging & constantly changing Threat Landscape
- Share the findings and **appropriate** solutions to help protect your Data

Intuity

ISO 27001
CERTIFICATION EUROPE ™

CYBER ESSENTIALS

CYBER | IRELAND
IRELAND'S CYBER SECURITY CLUSTER

MBA ASSOCIATION OF IRELAND

## Plan for today:

A Simple Framework

Cyber Threats 2021

State of Play (Irish Research)

Strategies for you

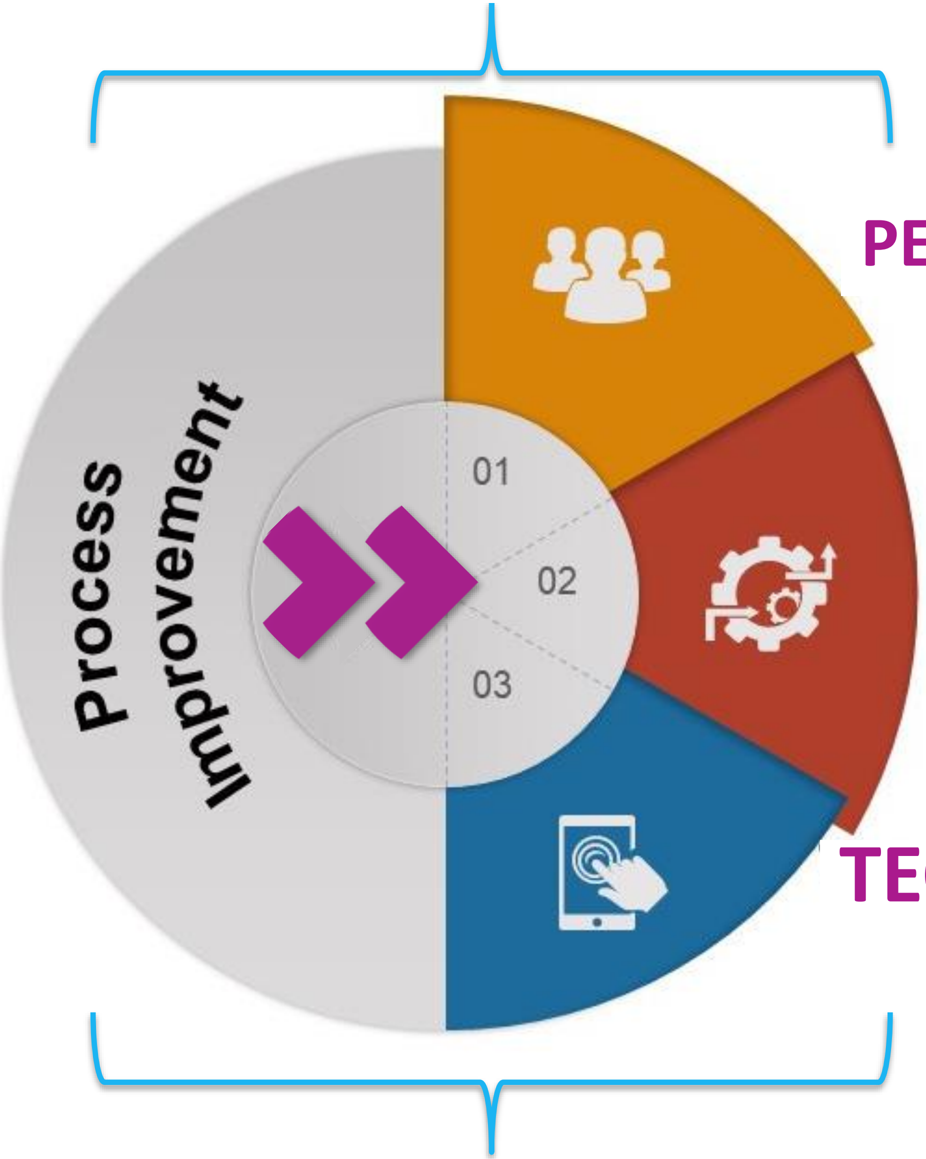
intuity

# Keep an eye out for this!

- Win a 1 hour CyberSecurity Training Session for your Team / Network
  - Question will be included in the post-event questionnaire

# A Simple Framework for Success

Your Business Strategy



Your Data

## PEOPLE

Is my organisation set up for success?

## PROCESS

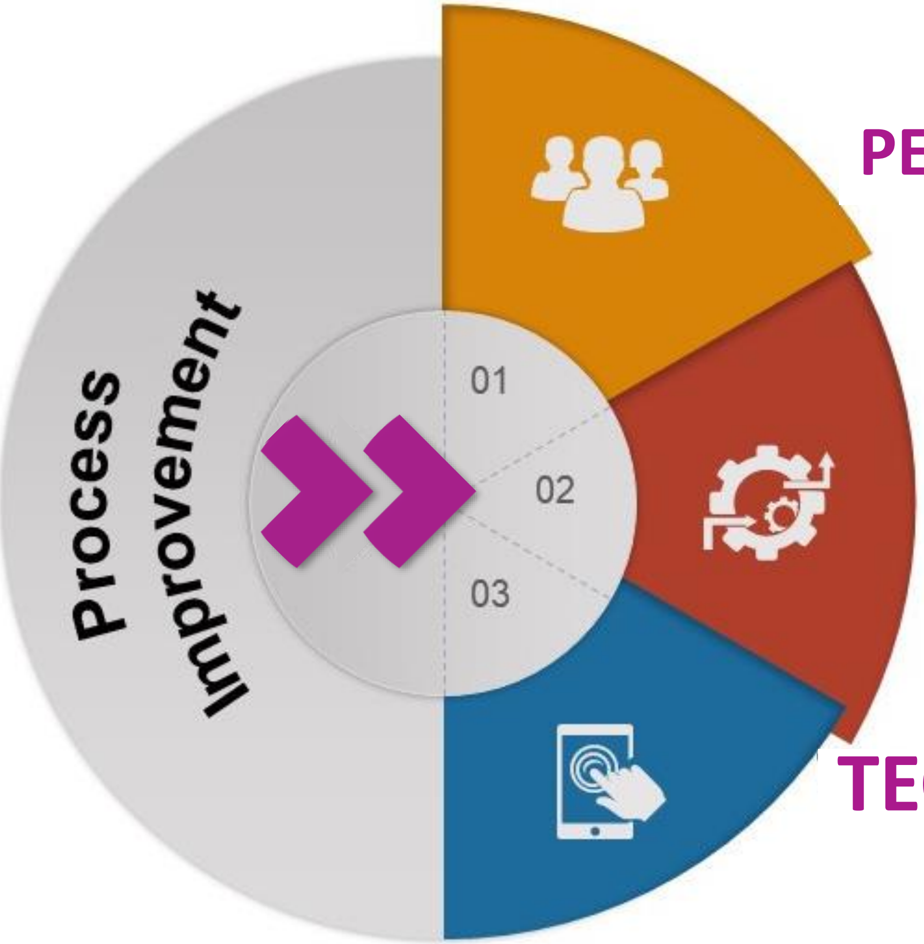
Are our processes aligned with our Business objectives?

## TECHNOLOGY

Are we leveraging the right Technology in the right way?

intuity

# A Simple Framework for Success



## PEOPLE

Is my organisation set up for success?

## PROCESS

Are our processes aligned with our Business objectives?

## TECHNOLOGY

Are we leveraging the right Technology in the right way?

# Cyber Threats

## Ever-changing threats and how to mitigate against them

# Cyber Threats

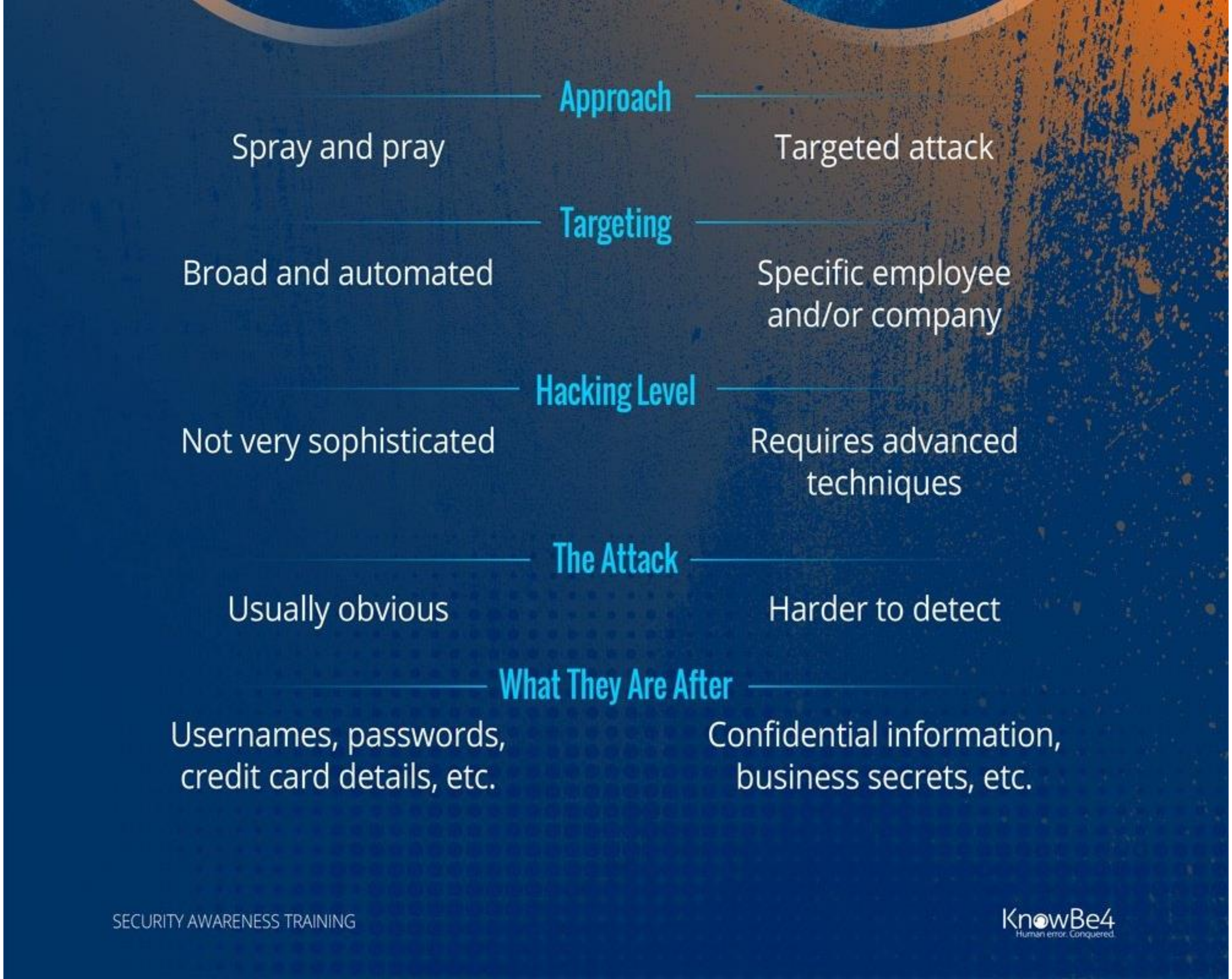
Spear Phishing

Mobile Vulnerabilities

Fileless Malware

Ransomware

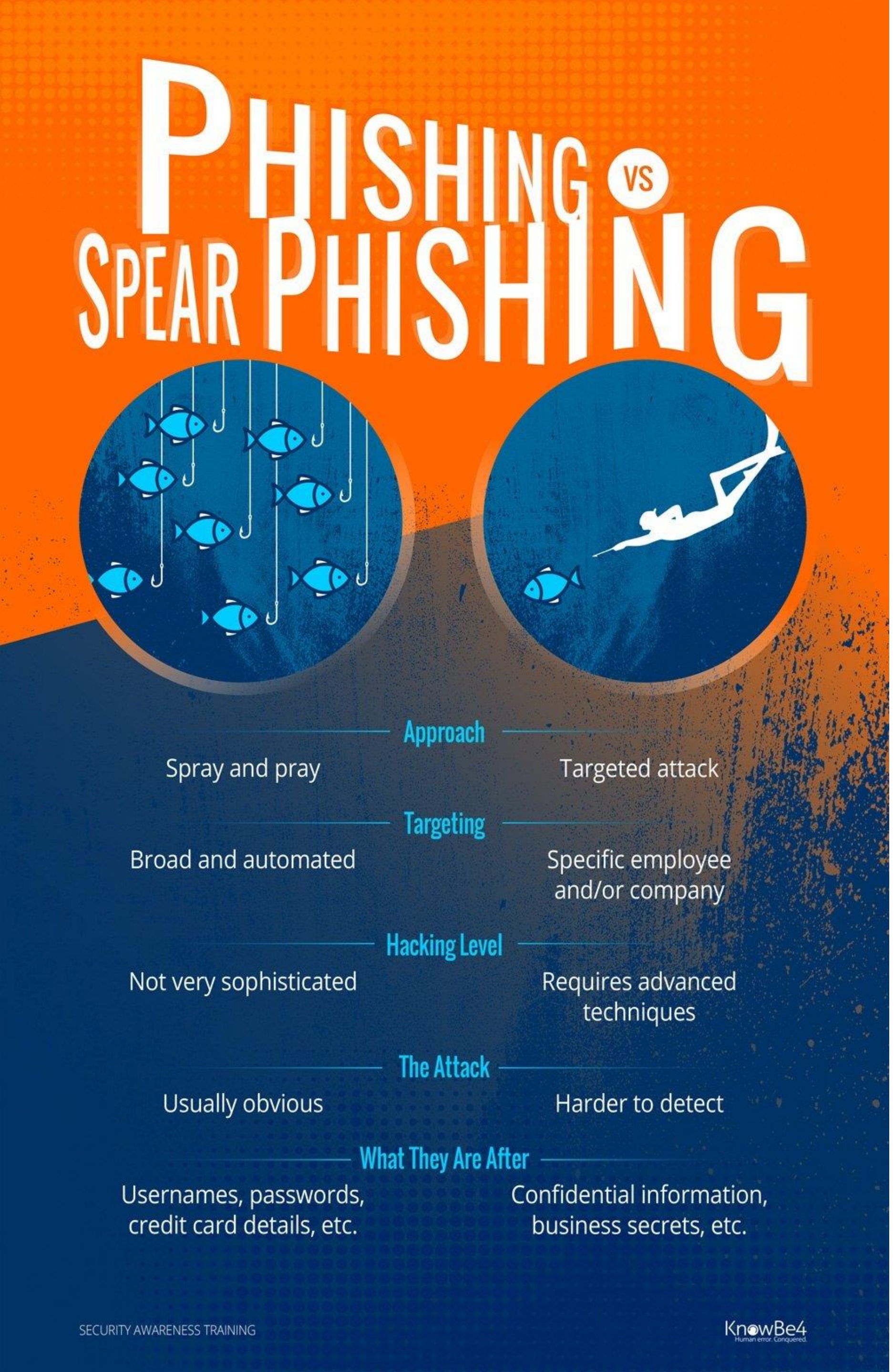
PHISHING
VS
SPEAR PHISHING



| | | |
|---|---|---|
| Approach | Spray and pray | Targeted attack |
| Targeting | Broad and automated | Specific employee and/or company |
| Hacking Level | Not very sophisticated | Requires advanced techniques |
| The Attack | Usually obvious | Harder to detect |
| What They Are After | Usernames, passwords, credit card details, etc. | Confidential information, business secrets, etc. |

SECURITY AWARENESS TRAINING

KnowBe4
Human error. Conquered.



| Phishing | | Spear Phishing |
|---|---|---|
| Spray and pray | Approach | Targeted attack |
| Broad and automated | Targeting | Specific employee and/or company |
| Not very sophisticated | Hacking Level | Requires advanced techniques |
| Usually obvious | The Attack | Harder to detect |
| Usernames, passwords, credit card details, etc. | What They Are After | Confidential information, business secrets, etc. |

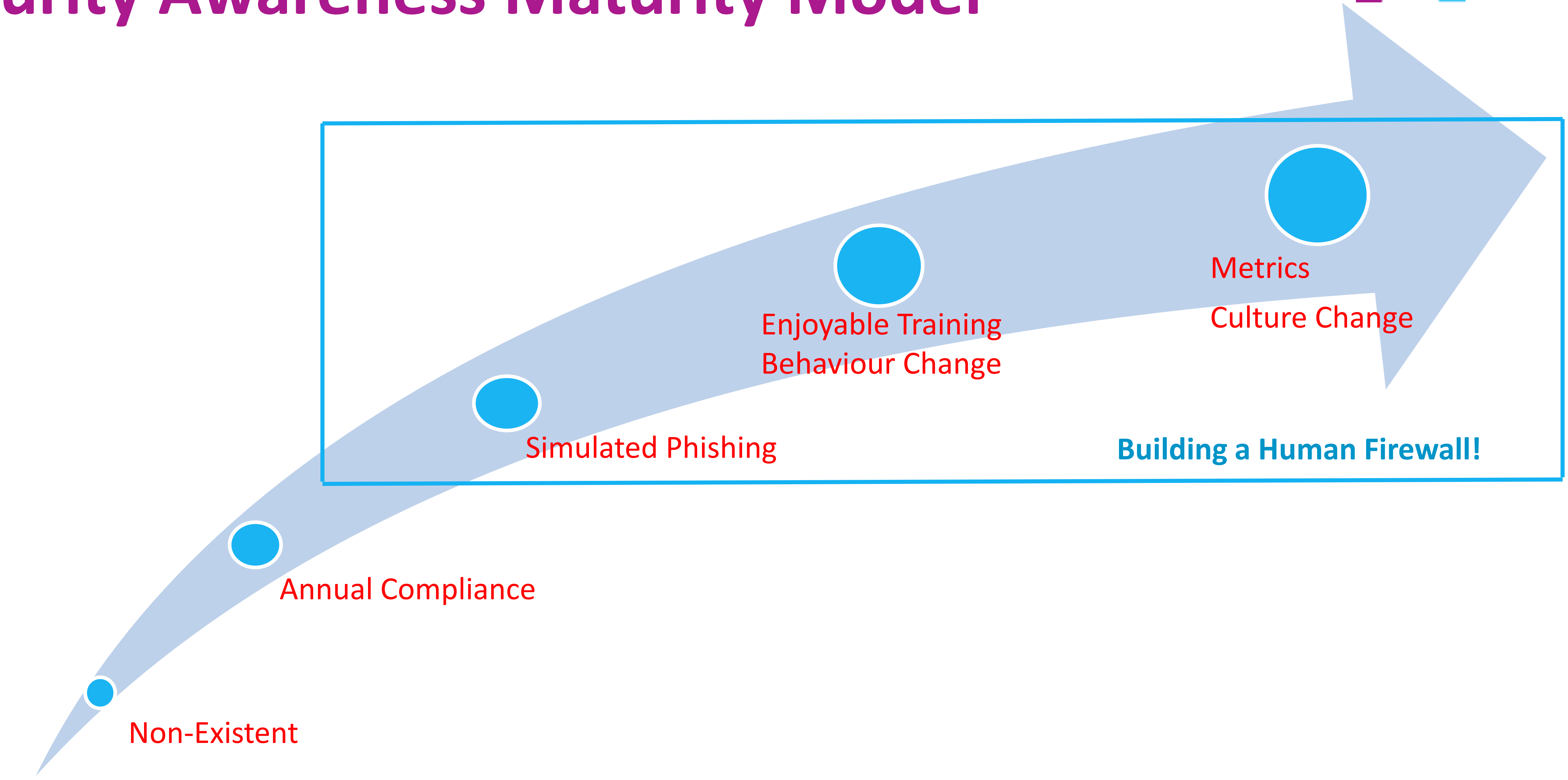
## Effectiveness * :

- Phishing 25%
- Spear Phishing 45%

## Solutions:

- **People:** Build your Human Firewall
  - Train & Simulate Phishing
- **Process:** Internet & Email usage policy
- **Technology:** Patching systems, Email protection, Spam filtering, link protection etc.

# Security Awareness Maturity Model



Non-Existent

Annual Compliance

Simulated Phishing

Enjoyable Training
Behaviour Change

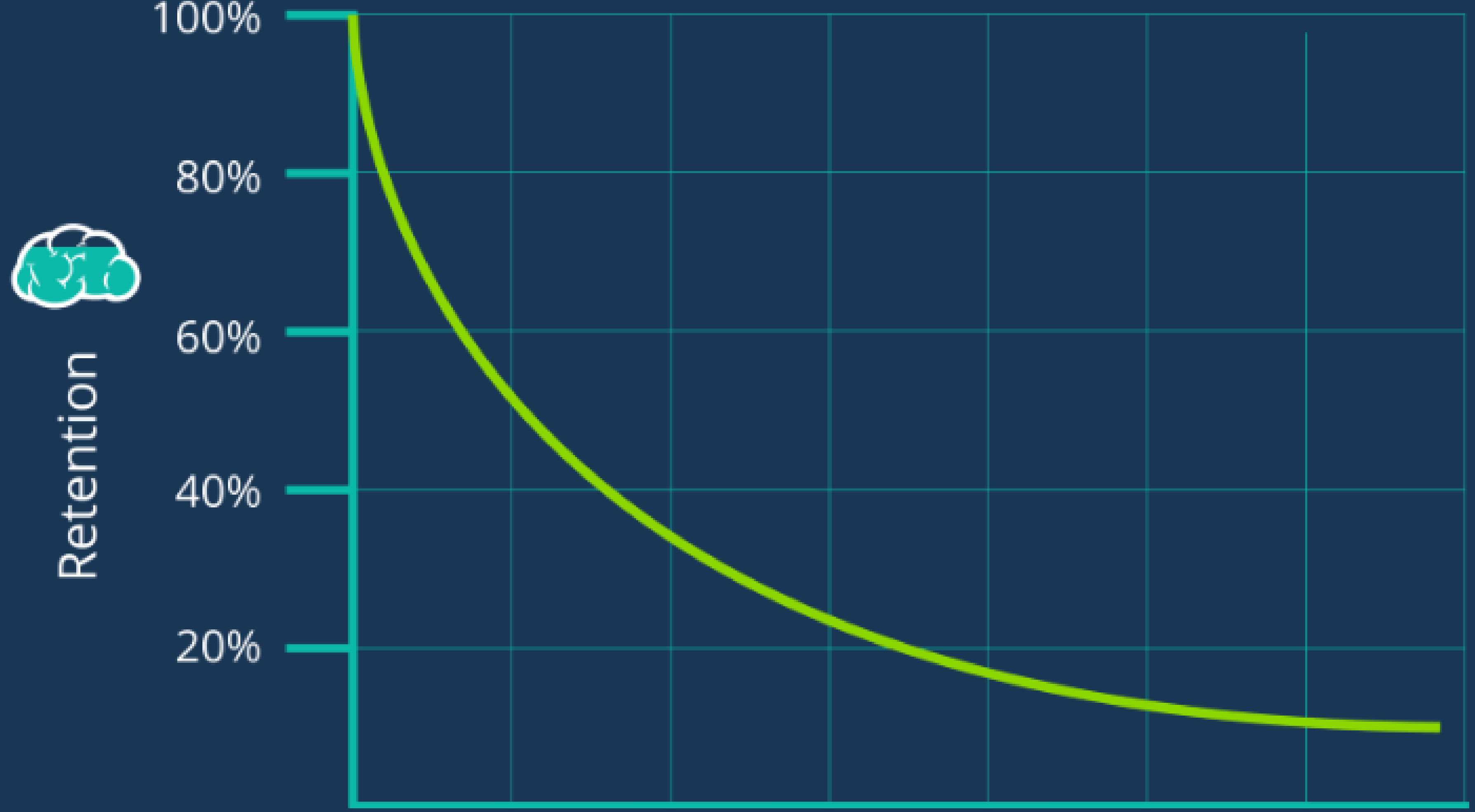
Metrics

Culture Change

**Building a Human Firewall!**

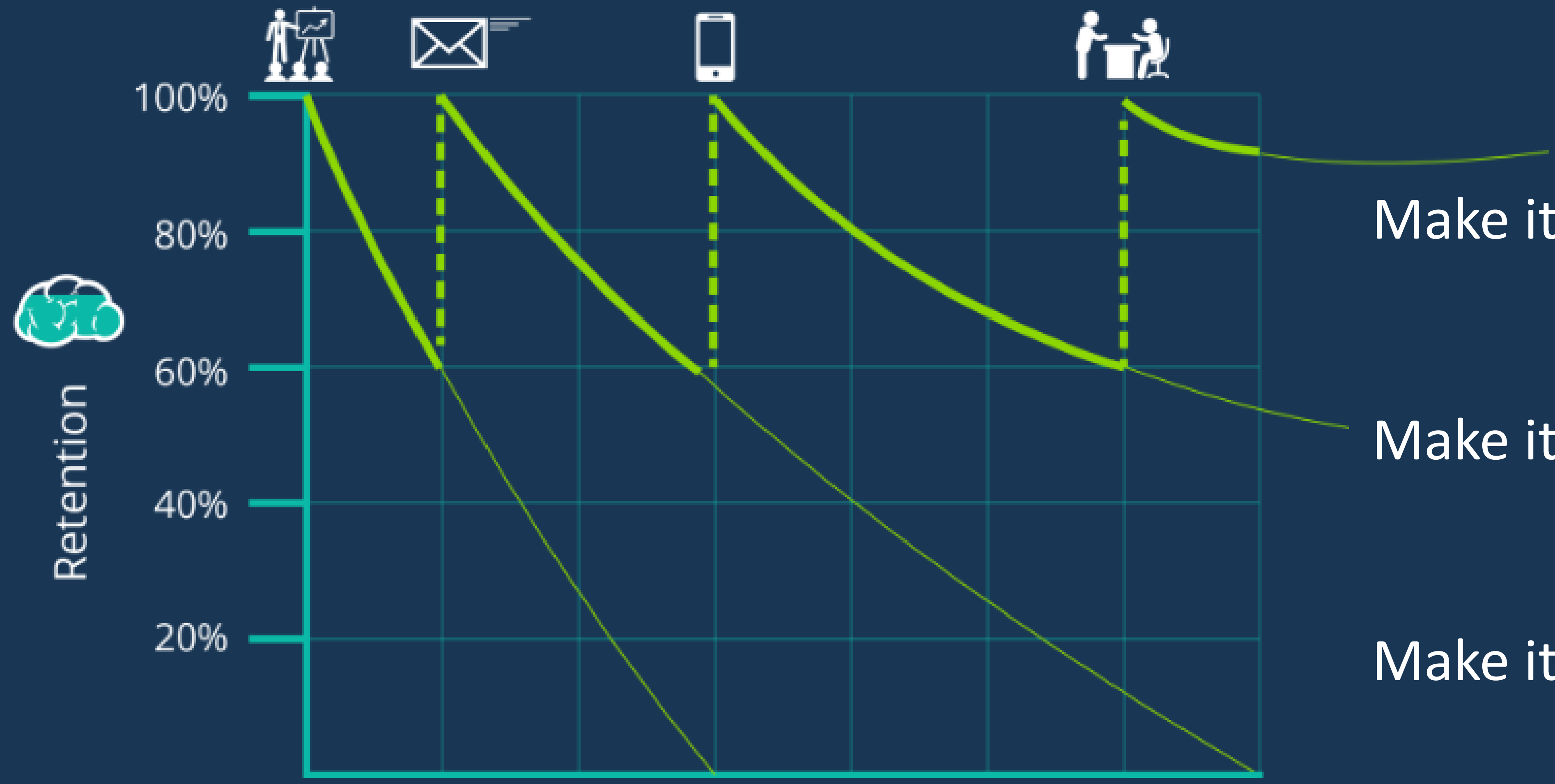
intuity

# THE FORGETTING CURVE



intuity

# COMBATING THE FORGETTING CURVE

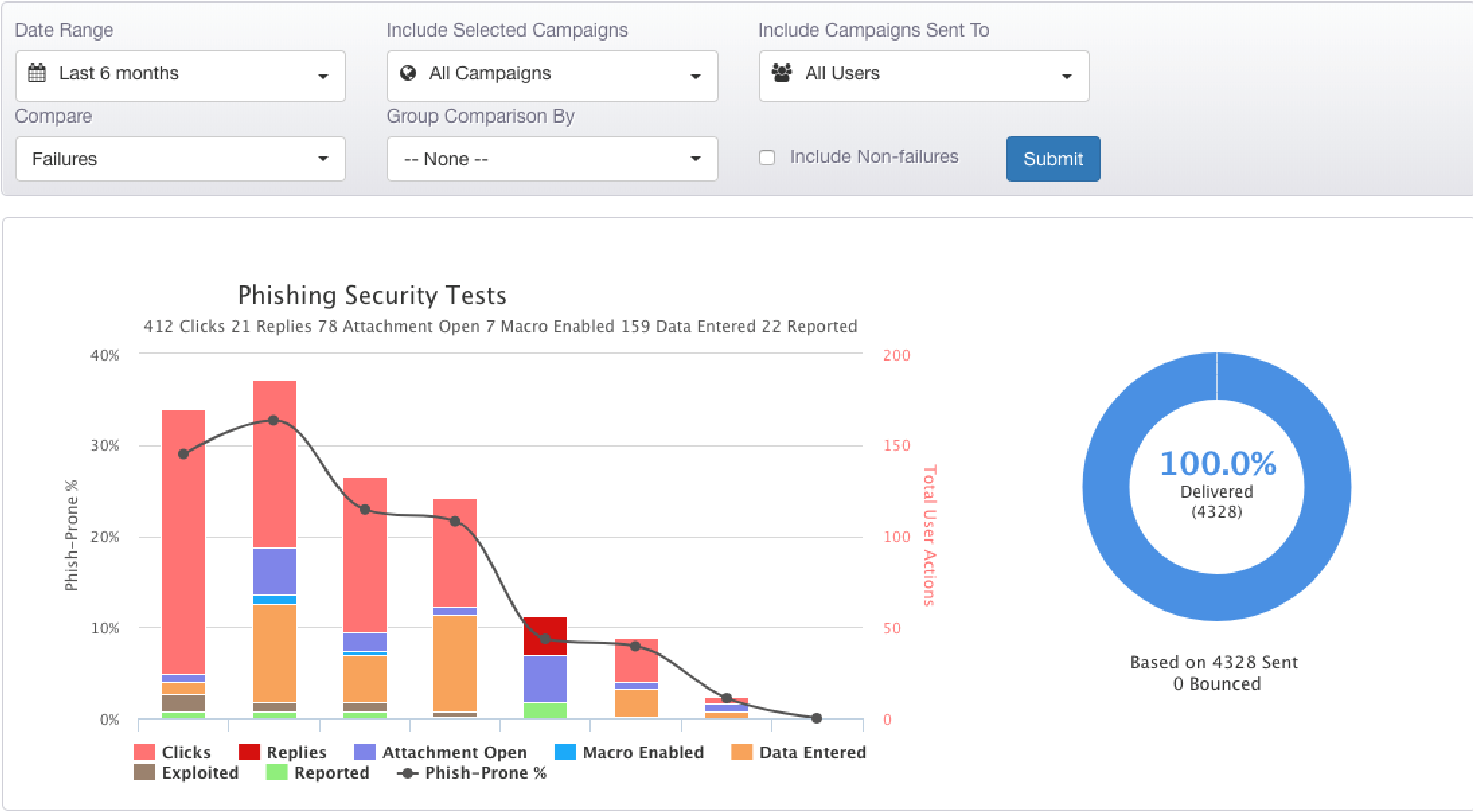


Make it interactive

Make it fun & engaging!

Make it relevant

Source: growthengineering.co.uk/what-is-the-forgetting-curve



Date Range: Last 6 months

Include Selected Campaigns: All Campaigns

Include Campaigns Sent To: All Users

Compare: Failures

Group Comparison By: -- None --

☐ Include Non-failures

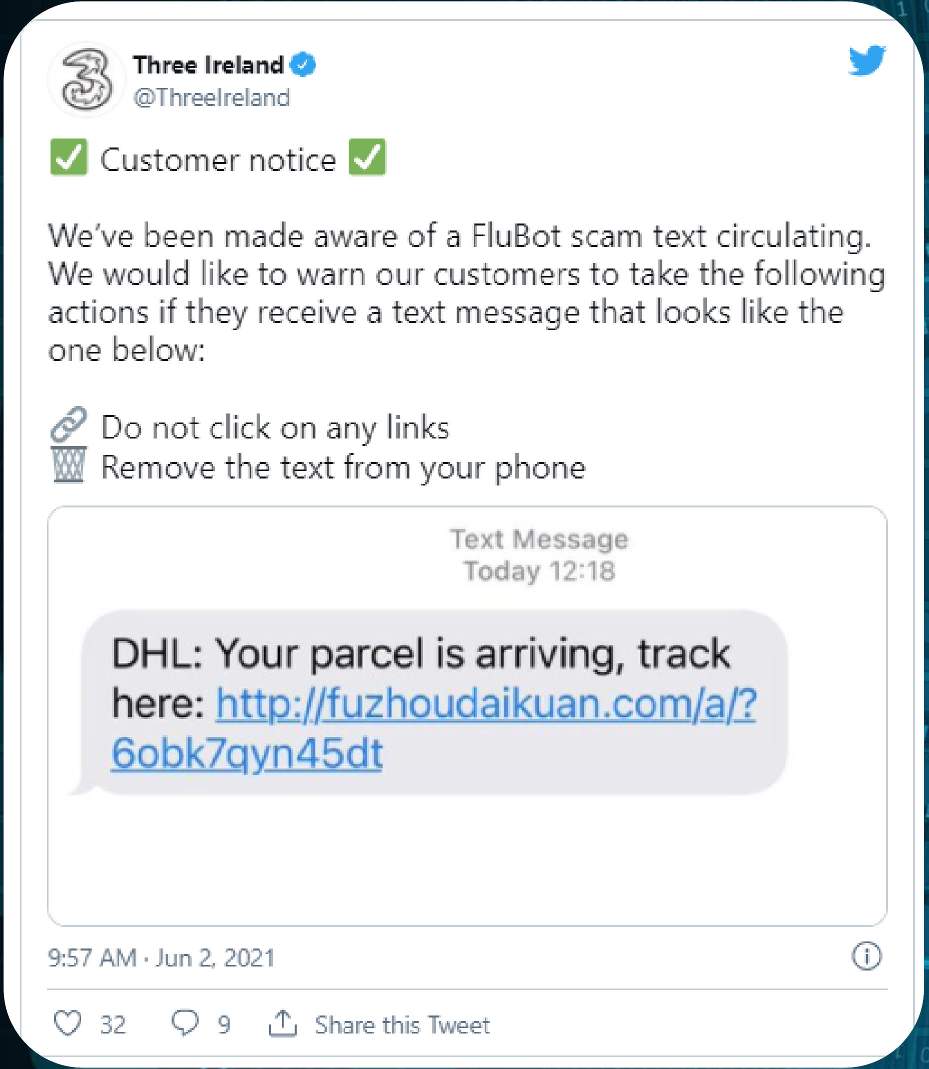
Submit

Phishing Security Tests

412 Clicks 21 Replies 78 Attachment Open 7 Macro Enabled 159 Data Entered 22 Reported

Based on 4328 Sent
0 Bounced

# FluBot – Mobile Vulnerabilities



Three Ireland
@ThreeIreland

✅ Customer notice ✅

We've been made aware of a FluBot scam text circulating. We would like to warn our customers to take the following actions if they receive a text message that looks like the one below:

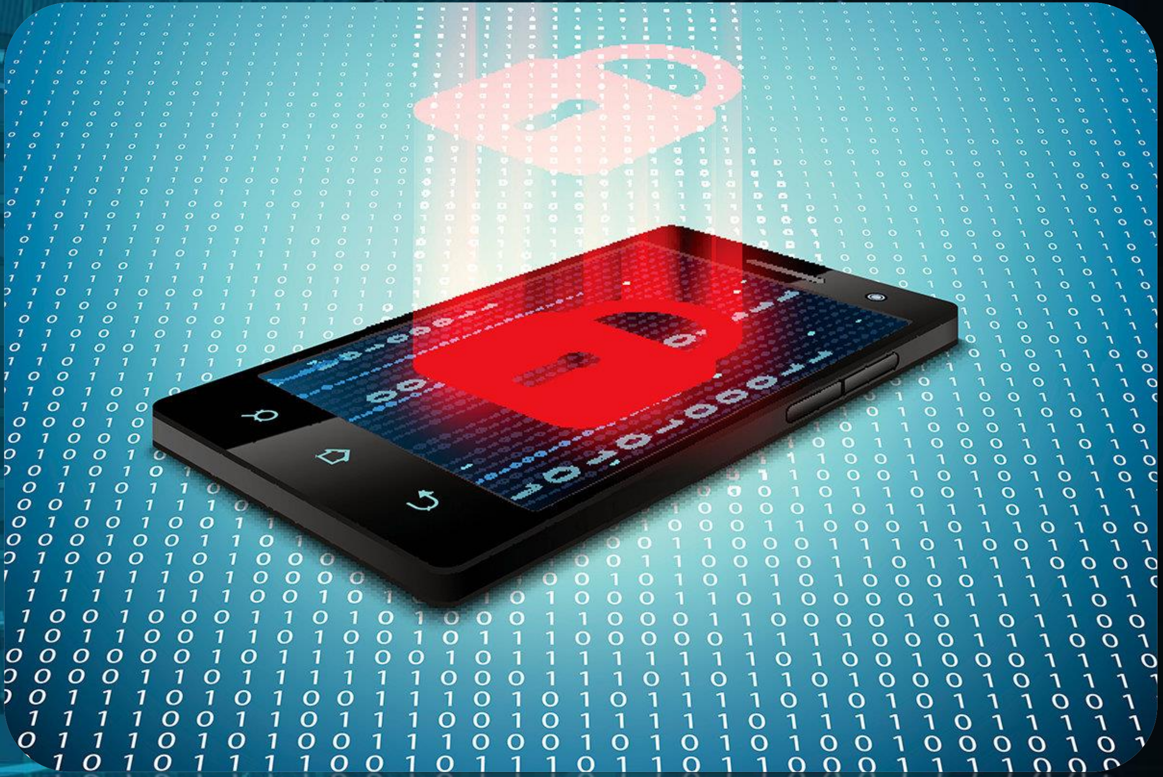
🔗 Do not click on any links
🗑 Remove the text from your phone

Text Message
Today 12:18

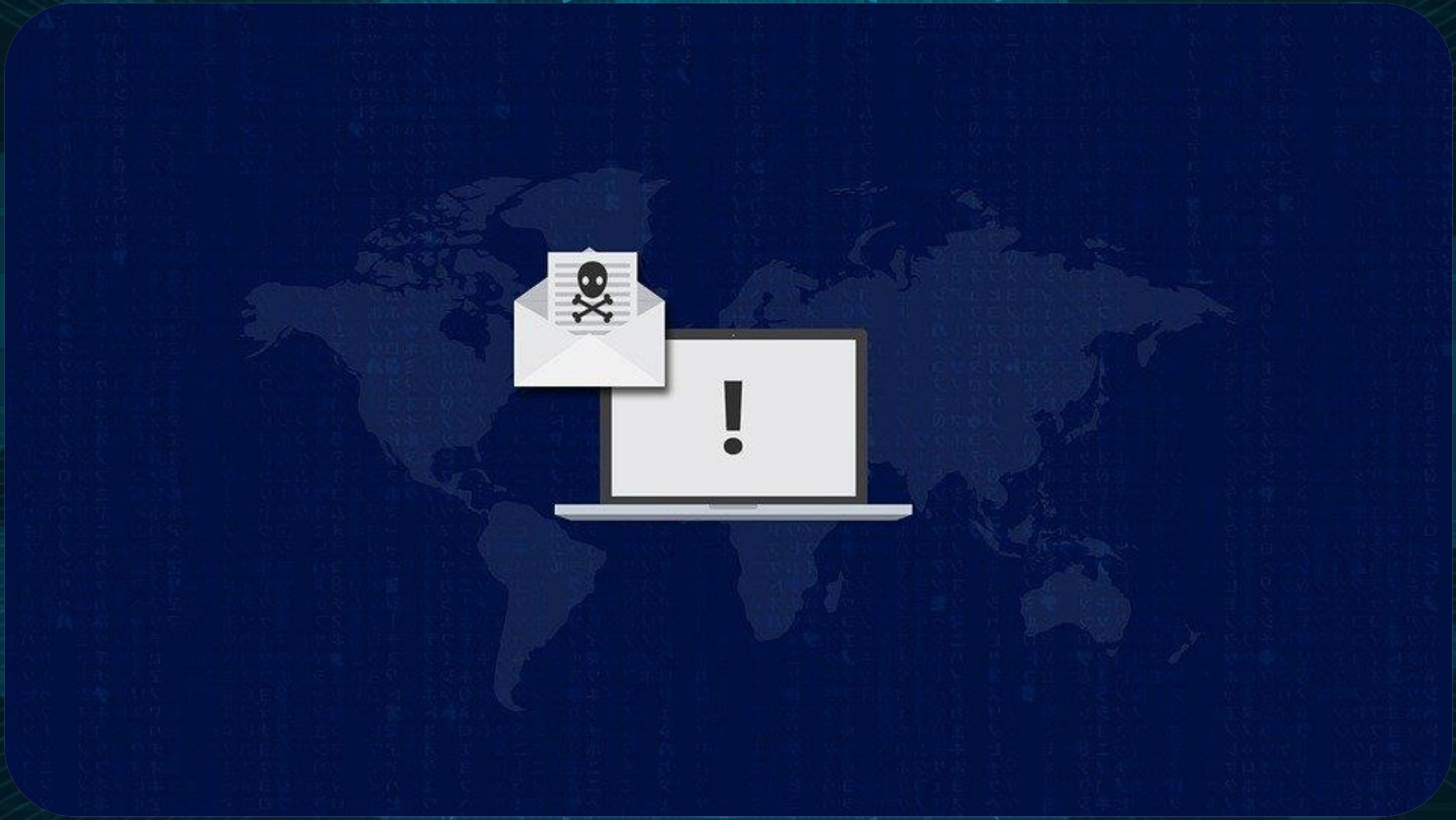
DHL: Your parcel is arriving, track here: http://fuzhoudaikuan.com/a/?6obk7qyn45dt

9:57 AM · Jun 2, 2021

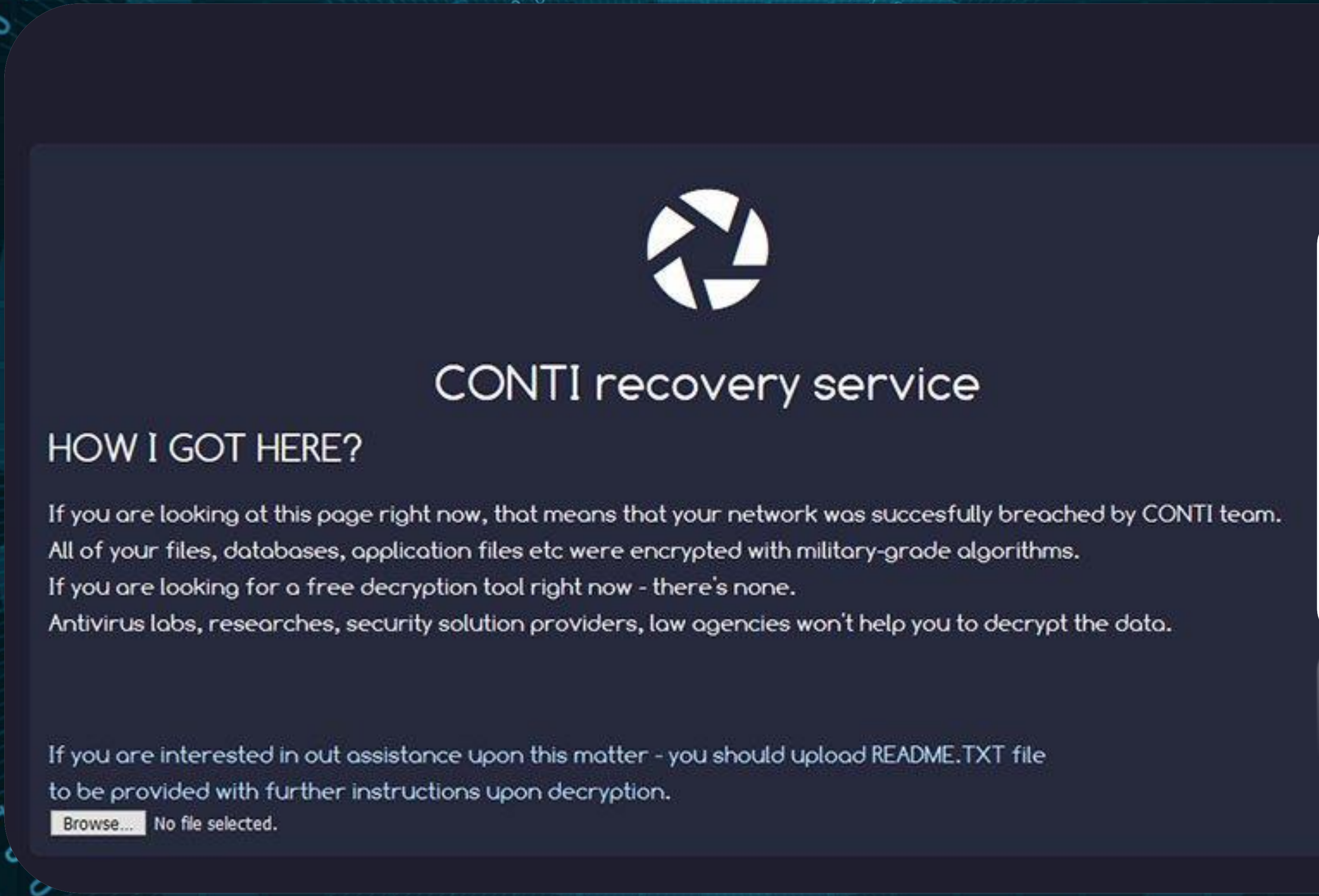
♡ 32 💬 9 Share this Tweet



# Fileless Malware



# RansomWare (e.g. Conti, WannaCry)



CONTI recovery service

HOW I GOT HERE?

If you are looking at this page right now, that means that your network was succesfully breached by CONTI team.
All of your files, databases, application files etc were encrypted with military-grade algorithms.
If you are looking for a free decryption tool right now - there's none.
Antivirus labs, researches, security solution providers, law agencies won't help you to decrypt the data.

If you are interested in out assistance upon this matter - you should upload README.TXT file
to be provided with further instructions upon decryption.

# Conti Ransomware

- “Double Extortion” Ransomware

- Restoring your Backups may not be enough to avoid the ransom / fines

intuity

SECURING THE

FUTURE

The Cyber Security Climate in Ireland

An Amárach report for Microsoft

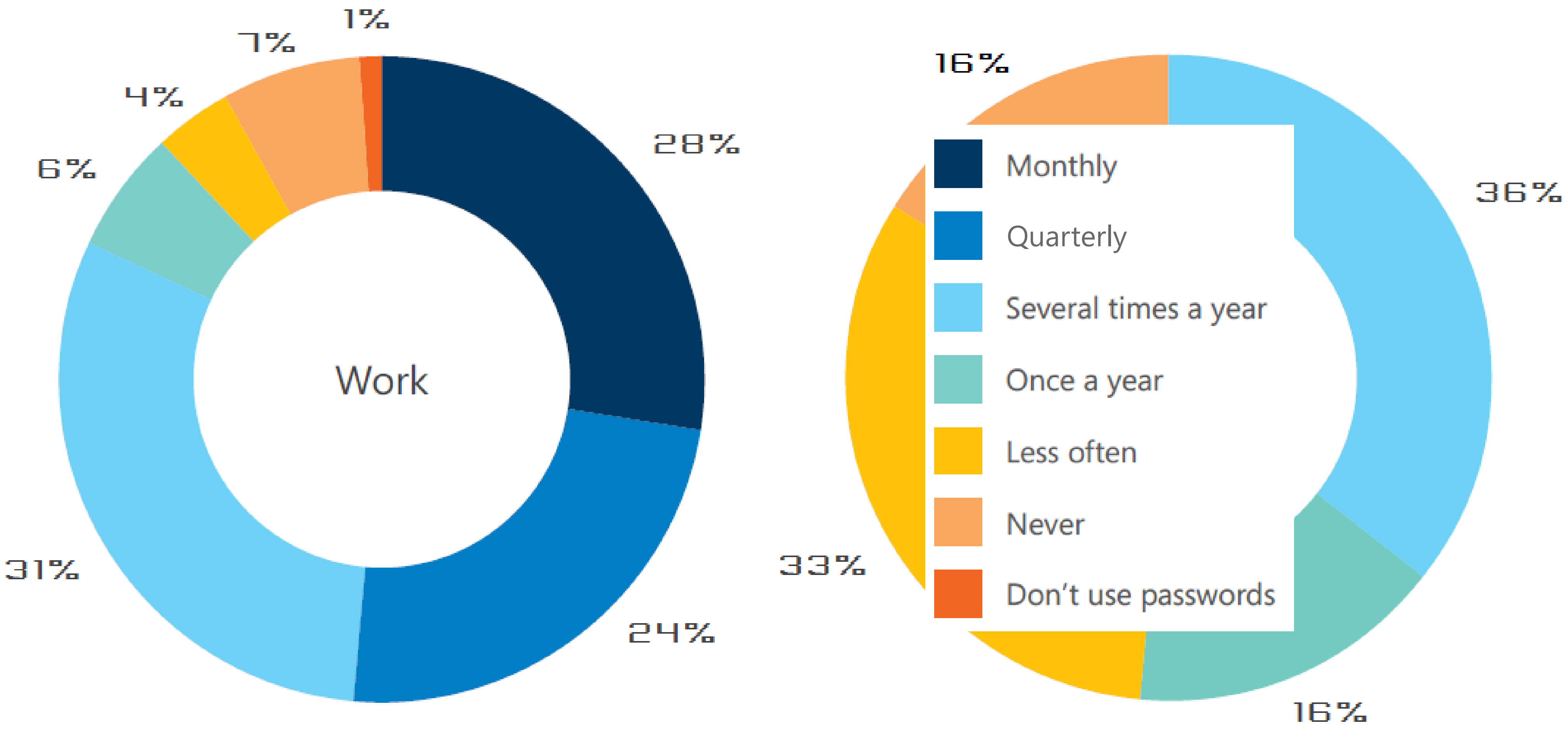
JANUARY 2019

Microsoft

Securing the Future 2020

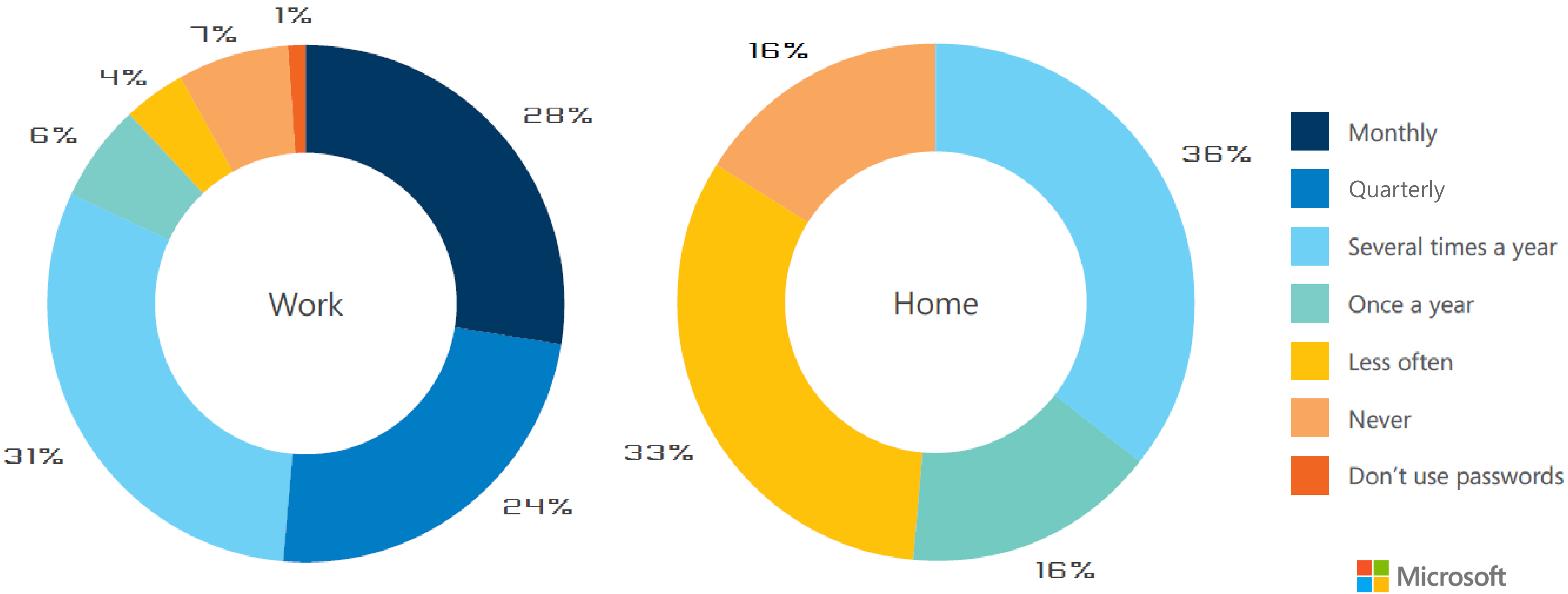
THE STATE OF CYBERSECURITY IN IRELAND
AN AMÁRACH REPORT FOR MICROSOFT IRELAND
JANUARY 2020

# How often do you change your passwords?



**77% of respondents rely on their memory to remember passwords**

# How often do you change your passwords?



Microsoft

intuity

**77% of respondents rely on their memory to remember passwords**

43% of public and private sector employees in Ireland using the same password across different technology.

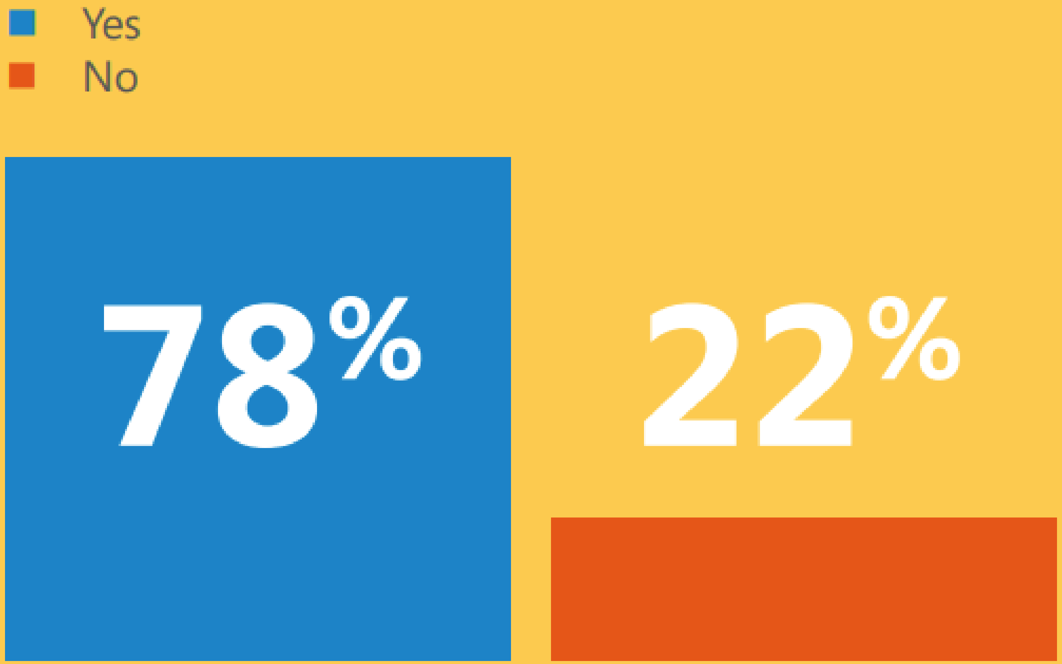
Microsoft

intuity

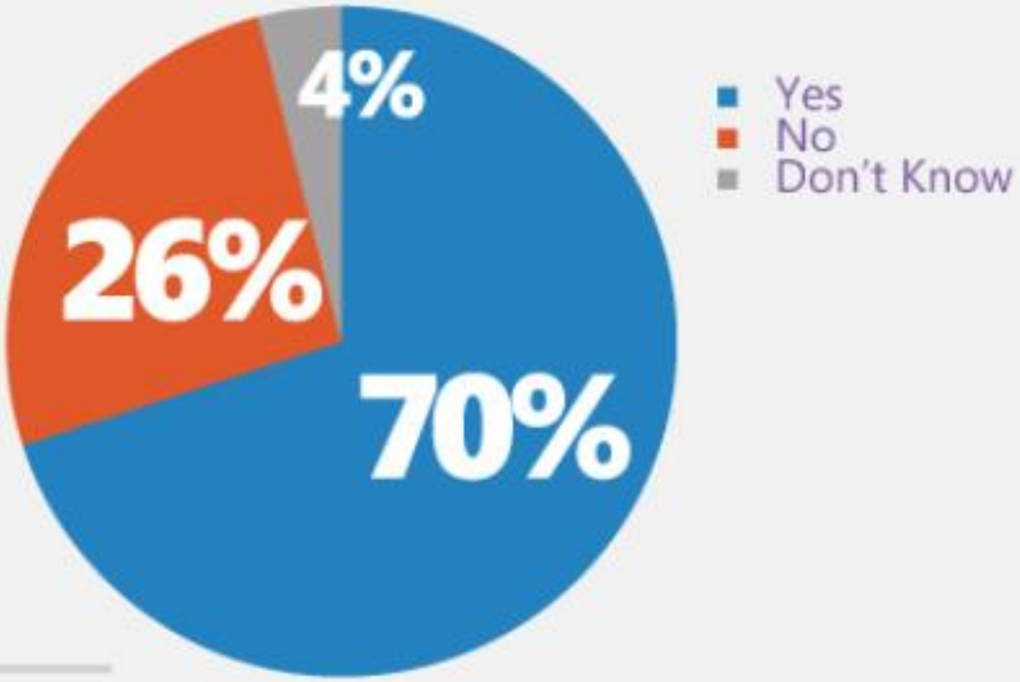
- Half

of users that work from home use their personal cloud services

# Does your organisation have restrictions on access to documents, email or other imformation relating to work when working from home?

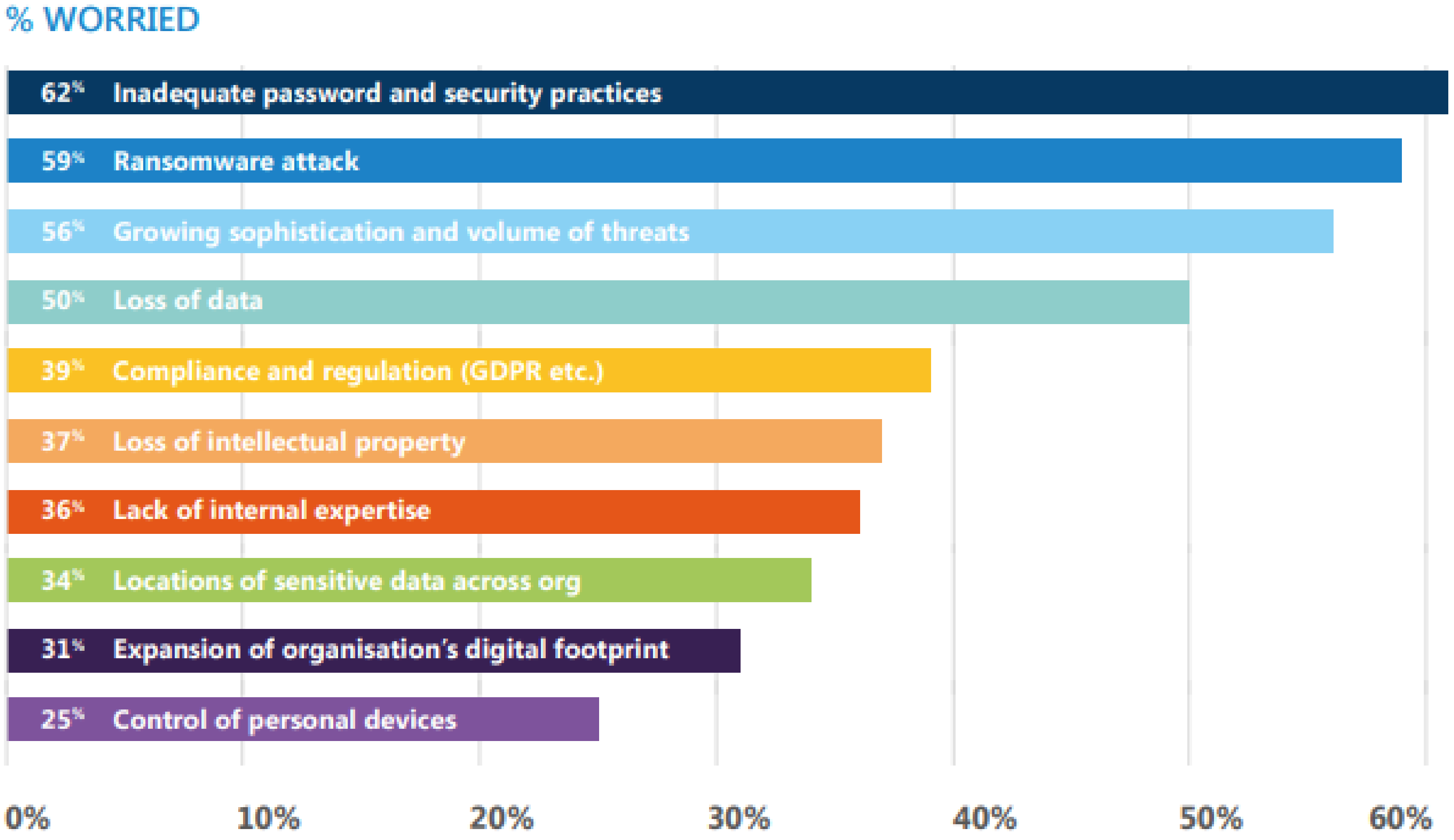


# Has your organisation ever experienced problems with phishing, hacking, cyberfraud or other cyberattacks?



1 in 4 companies are confident they can respond to any security incident effectively.

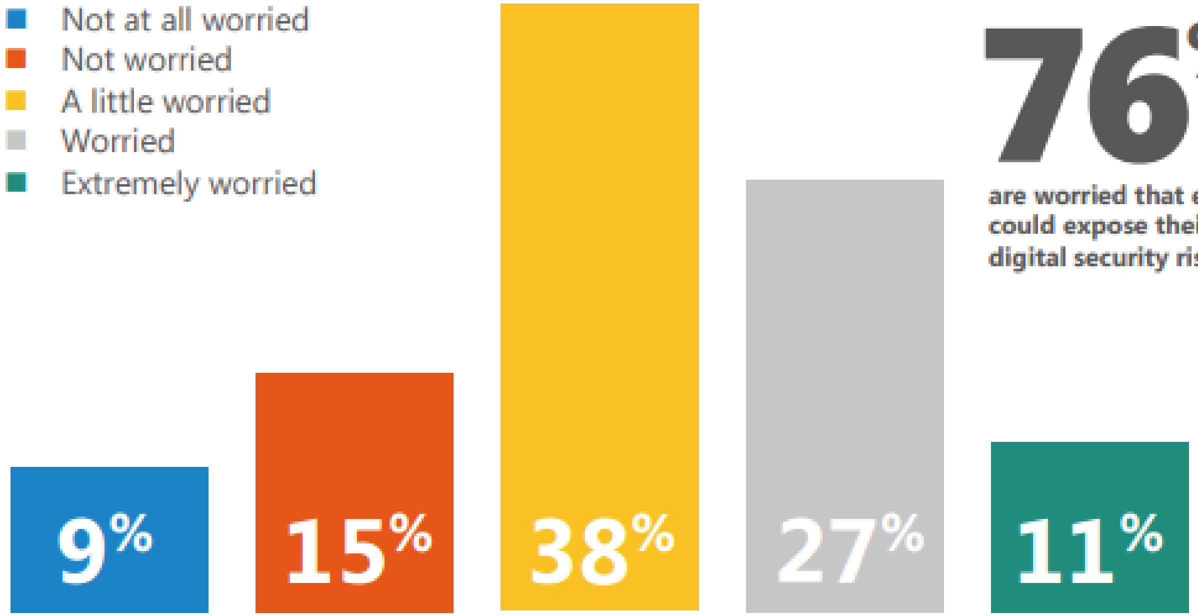
# Main security threat concerns for organisations in Ireland:



Microsoft

intuity

# How worried are you that your employees could expose your company to digital secruity risks?

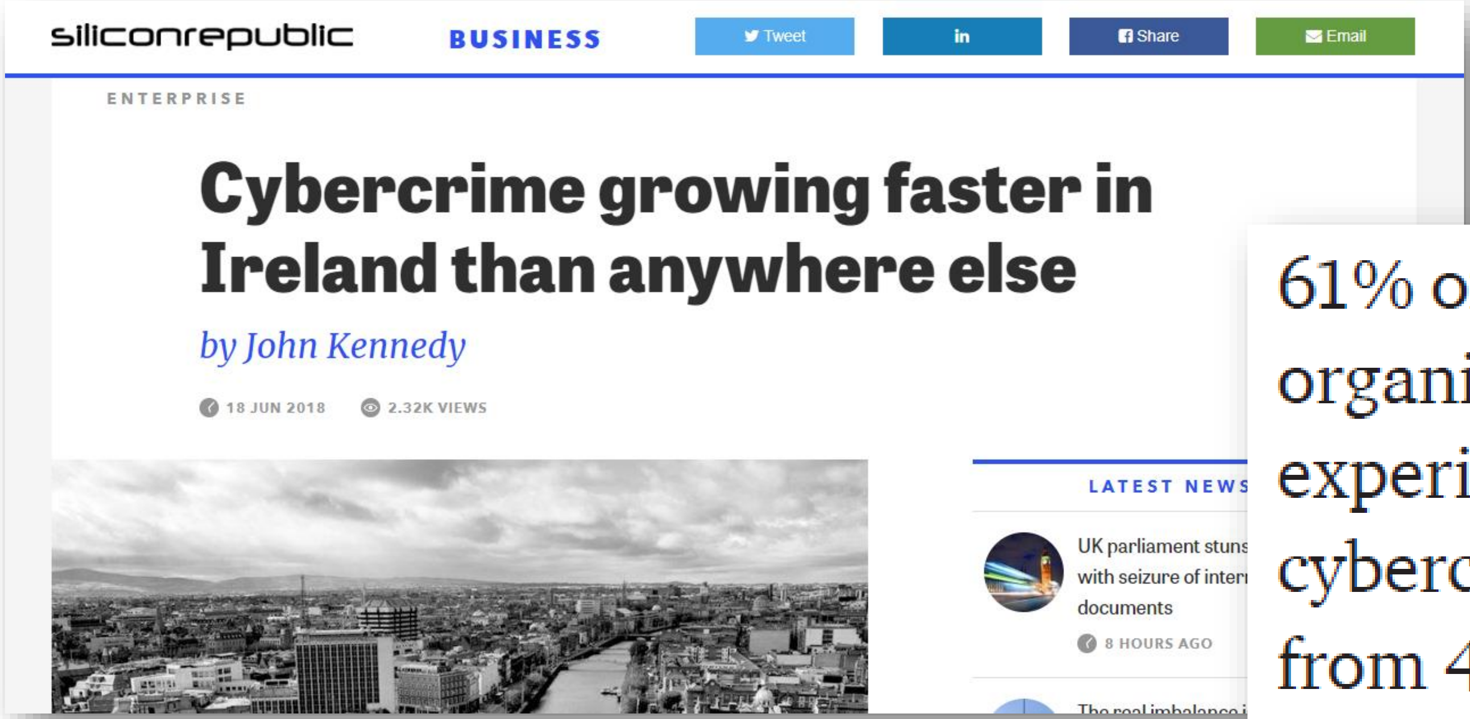


**76%**

**are worried that employees could expose their company to digital security risks**

42,000

# This impacts us all



siliconrepublic BUSINESS

Tweet in Share Email

ENTERPRISE

## Cybercrime growing faster in Ireland than anywhere else

*by John Kennedy*

18 JUN 2018 2.32K VIEWS

LATEST NEWS

UK parliament stuns with seizure of inter documents

8 HOURS AGO

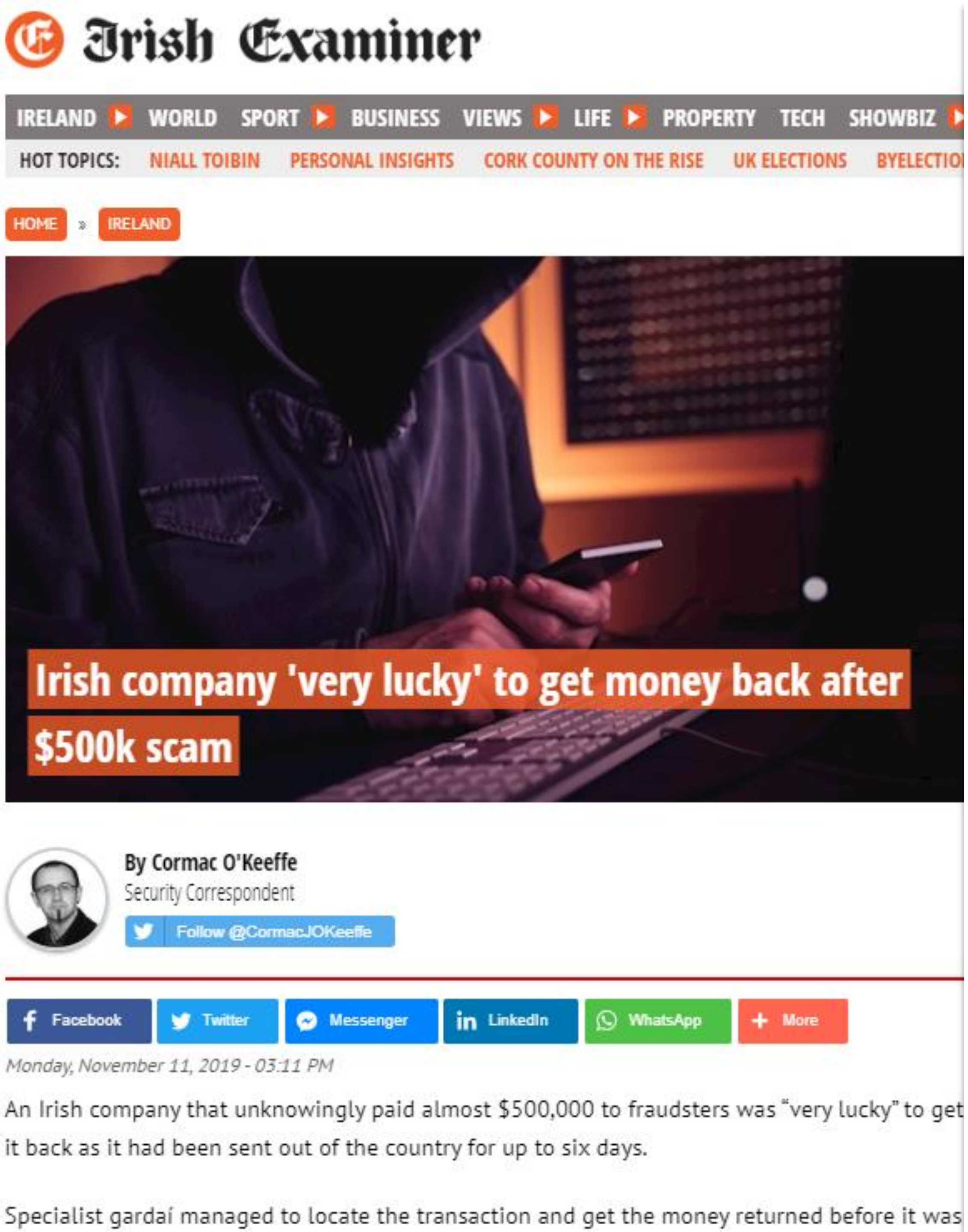
The real imbalance i

61% of Irish organisations experienced cybercrime, up from 44%

*"Here at the Garda National Cybercrime bureau we have seen a significant increase in the number of Ransomware attacks in 2021."*

Source: pwc Irish Economic Crime Survey & Silicon Republic

intuity



Irish Examiner

# Irish company 'very lucky' to get money back after $500k scam

By Cormac O'Keeffe
Security Correspondent

Monday, November 11, 2019 - 03:11 PM

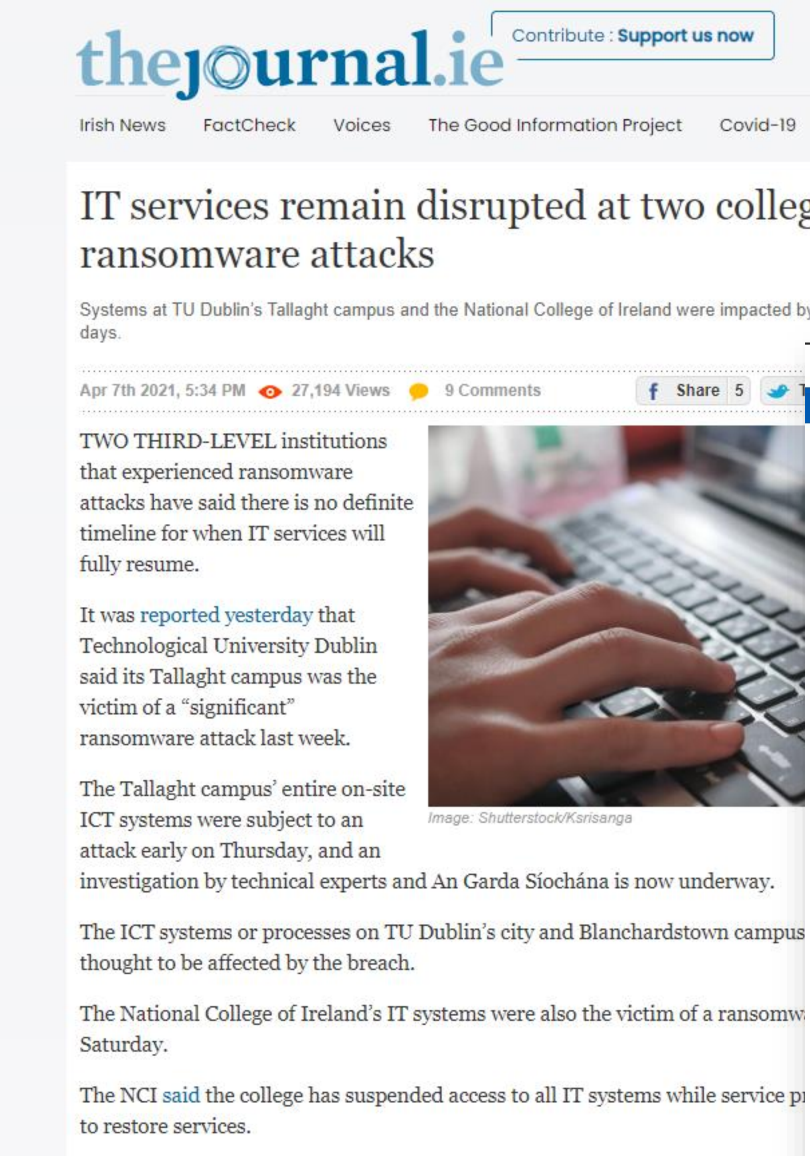
An Irish company that unknowingly paid almost $500,000 to fraudsters was "very lucky" to get it back as it had been sent out of the country for up to six days.

Specialist gardaí managed to locate the transaction and get the money returned before it was

- *"There has been a noticeable increase in what is known as* ***Invoice Redirect Fraud."***

- *"An awful lot of companies have been hit in the last few weeks,"*

- *"We are getting a couple of cases every week now."*



thejournal.ie

Contribute : **Support us now**

Irish News FactCheck Voices The Good Information Project Covid-19

## IT services remain disrupted at two colleges after ransomware attacks

Systems at TU Dublin's Tallaght campus and the National College of Ireland were impacted by attacks in recent days.

Apr 7th 2021, 5:34 PM 27,194 Views 9 Comments Share 5

TWO THIRD-LEVEL institutions that experienced ransomware attacks have said there is no definite timeline for when IT services will fully resume.

It was reported yesterday that Technological University Dublin said its Tallaght campus was the victim of a "significant" ransomware attack last week.

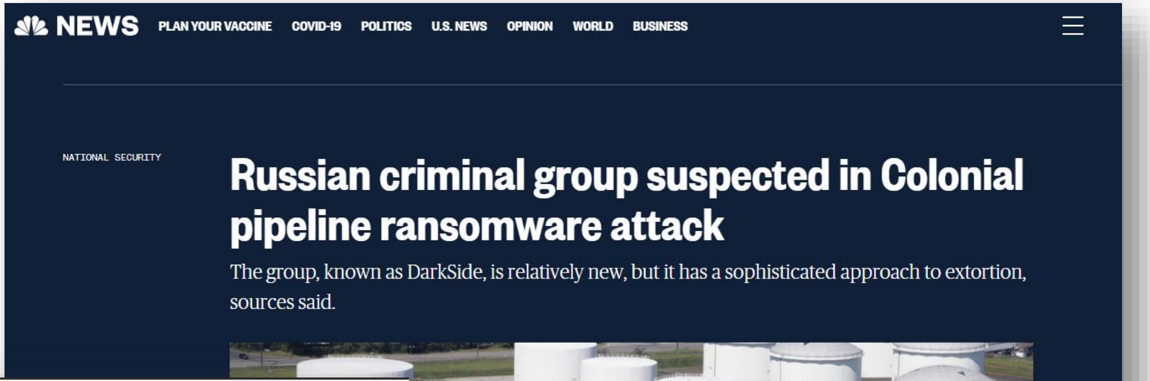
*Image: Shutterstock/Ksrisanga*

The Tallaght campus' entire on-site ICT systems were subject to an attack early on Thursday, and an investigation by technical experts and An Garda Síochána is now underway.

The ICT systems or processes on TU Dublin's city and Blanchardstown campus thought to be affected by the breach.

The National College of Ireland's IT systems were also the victim of a ransomw Saturday.

The NCI said the college has suspended access to all IT systems while service pr to restore services.

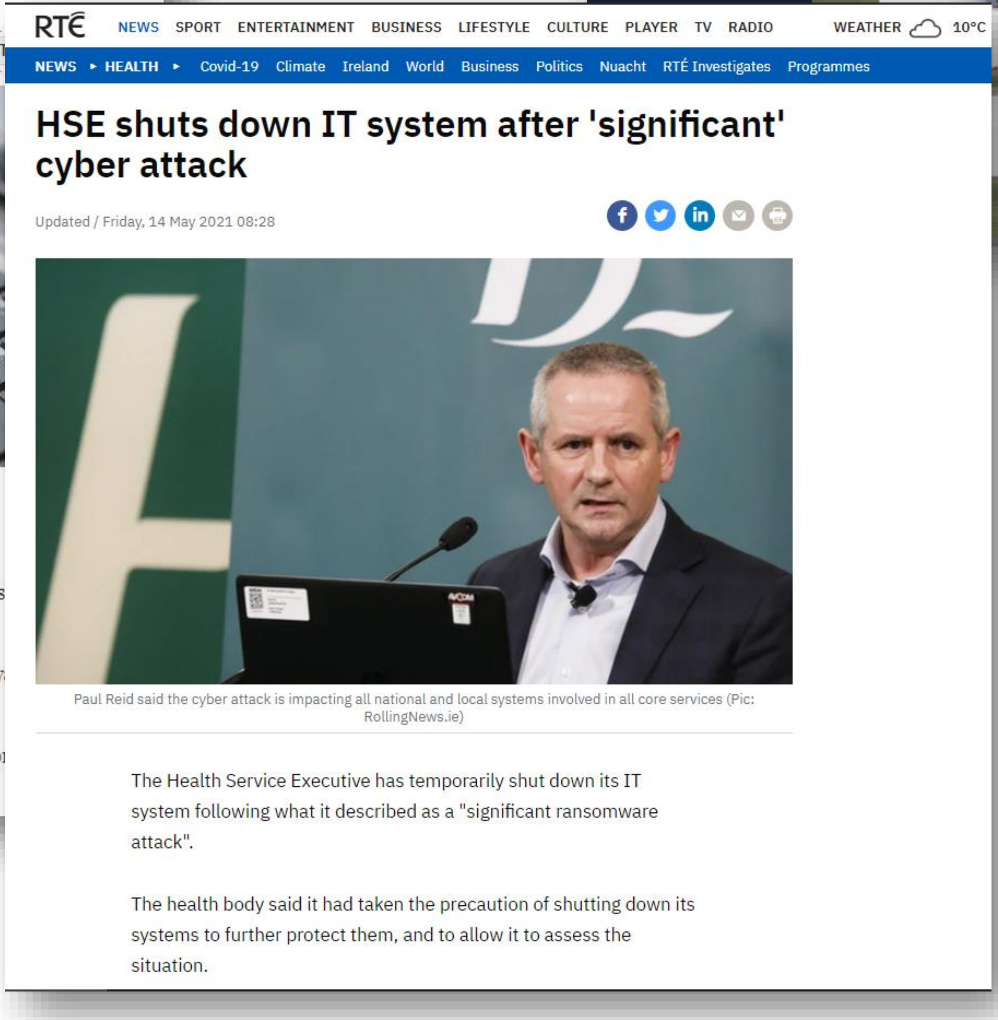


NEWS PLAN YOUR VACCINE COVID-19 POLITICS U.S. NEWS OPINION WORLD BUSINESS

NATIONAL SECURITY

## Russian criminal group suspected in Colonial pipeline ransomware attack

The group, known as DarkSide, is relatively new, but it has a sophisticated approach to extortion, sources said.



RTÉ NEWS SPORT ENTERTAINMENT BUSINESS LIFESTYLE CULTURE PLAYER TV RADIO WEATHER 10°C

NEWS ▸ HEALTH ▸ Covid-19 Climate Ireland World Business Politics Nuacht RTÉ Investigates Programmes

## HSE shuts down IT system after 'significant' cyber attack

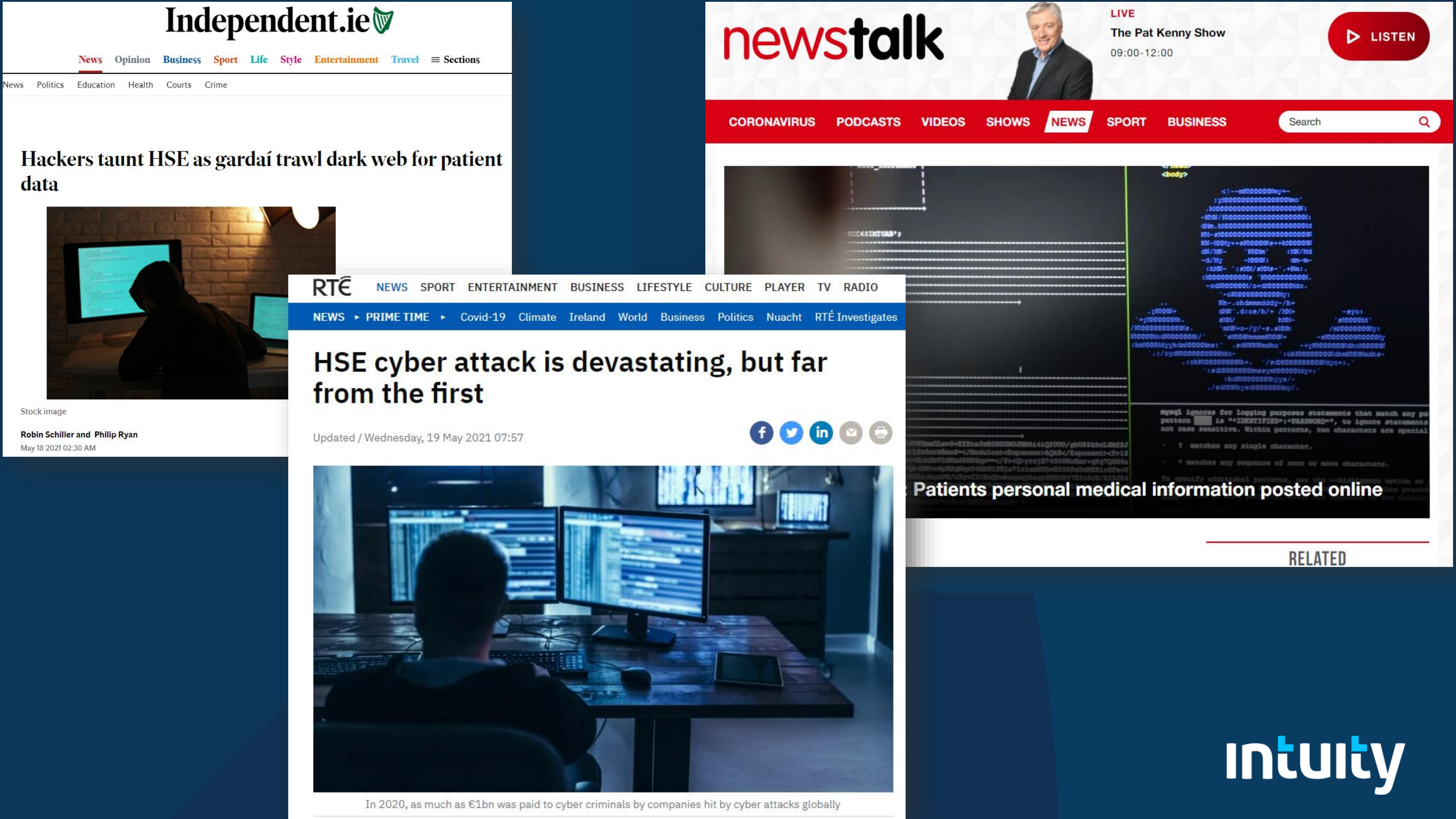
Updated / Friday, 14 May 2021 08:28

Paul Reid said the cyber attack is impacting all national and local systems involved in all core services (Pic: RollingNews.ie)

The Health Service Executive has temporarily shut down its IT system following what it described as a "significant ransomware attack".

The health body said it had taken the precaution of shutting down its systems to further protect them, and to allow it to assess the situation.

intuity



## Hackers taunt HSE as gardaí trawl dark web for patient data

Stock image

Robin Schiller and Philip Ryan

May 18 2021 02:30 AM

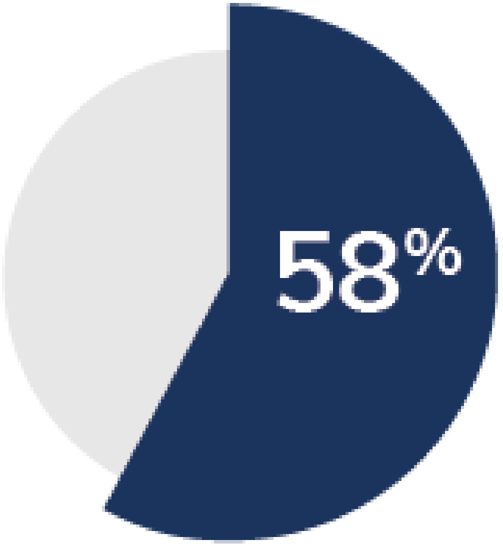
Patients personal medical information posted online

## HSE cyber attack is devastating, but far from the first

Updated / Wednesday, 19 May 2021 07:57

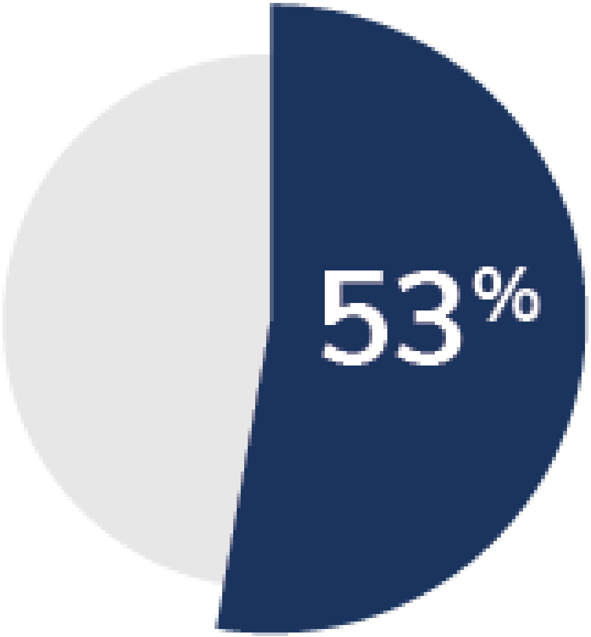
In 2020, as much as €1bn was paid to cyber criminals by companies hit by cyber attacks globally

intuity

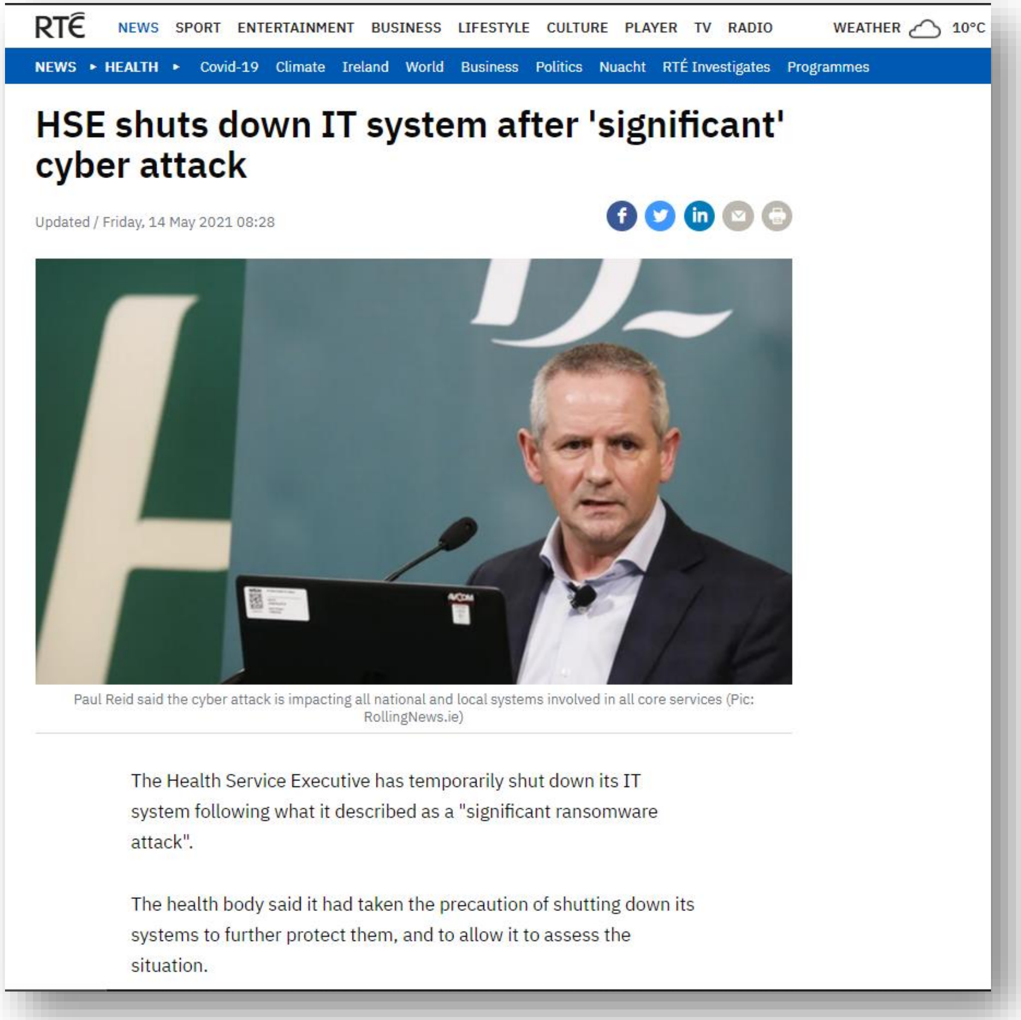


of Data Breaches in 2019 were small businesses

Small Businesses that would be unprofitable within one month if effected:



# Why this matters…


RTÉ
NEWS SPORT ENTERTAINMENT BUSINESS LIFESTYLE CULTURE PLAYER TV RADIO
WEATHER 10°C
NEWS ▸ HEALTH ▸ Covid-19 Climate Ireland World Business Politics Nuacht RTÉ Investigates Programmes

## HSE shuts down IT system after 'significant' cyber attack

Updated / Friday, 14 May 2021 08:28

Paul Reid said the cyber attack is impacting all national and local systems involved in all core services (Pic: RollingNews.ie)

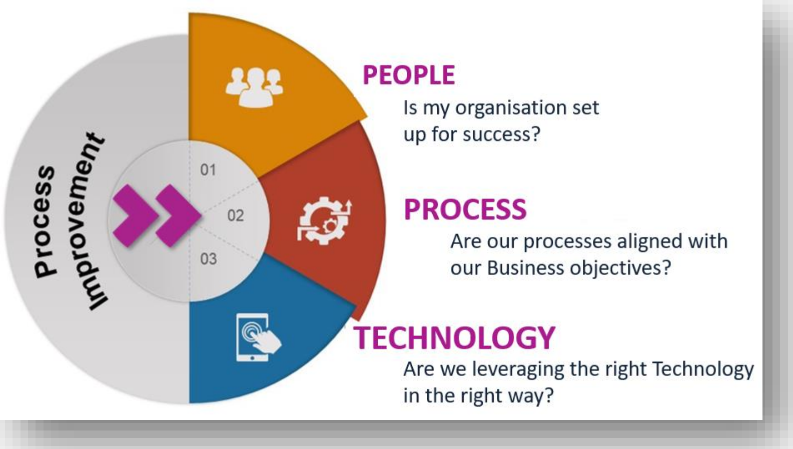
The Health Service Executive has temporarily shut down its IT system following what it described as a "significant ransomware attack".

The health body said it had taken the precaution of shutting down its systems to further protect them, and to allow it to assess the situation.

↔

# Our Top Recommendations

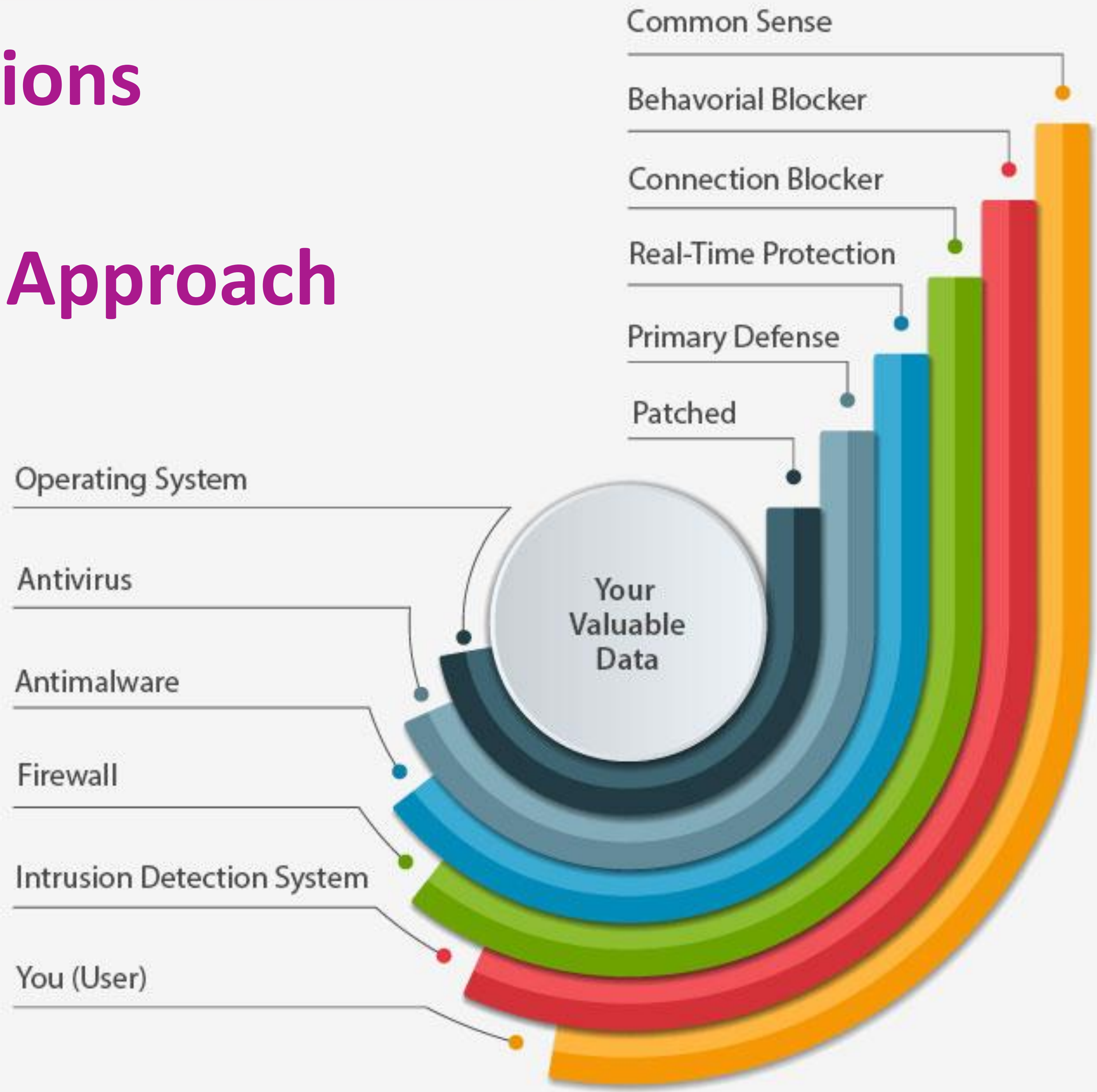
# Multi-Layered Security Approach



**PEOPLE**
Is my organisation set up for success?

**PROCESS**
Are our processes aligned with our Business objectives?

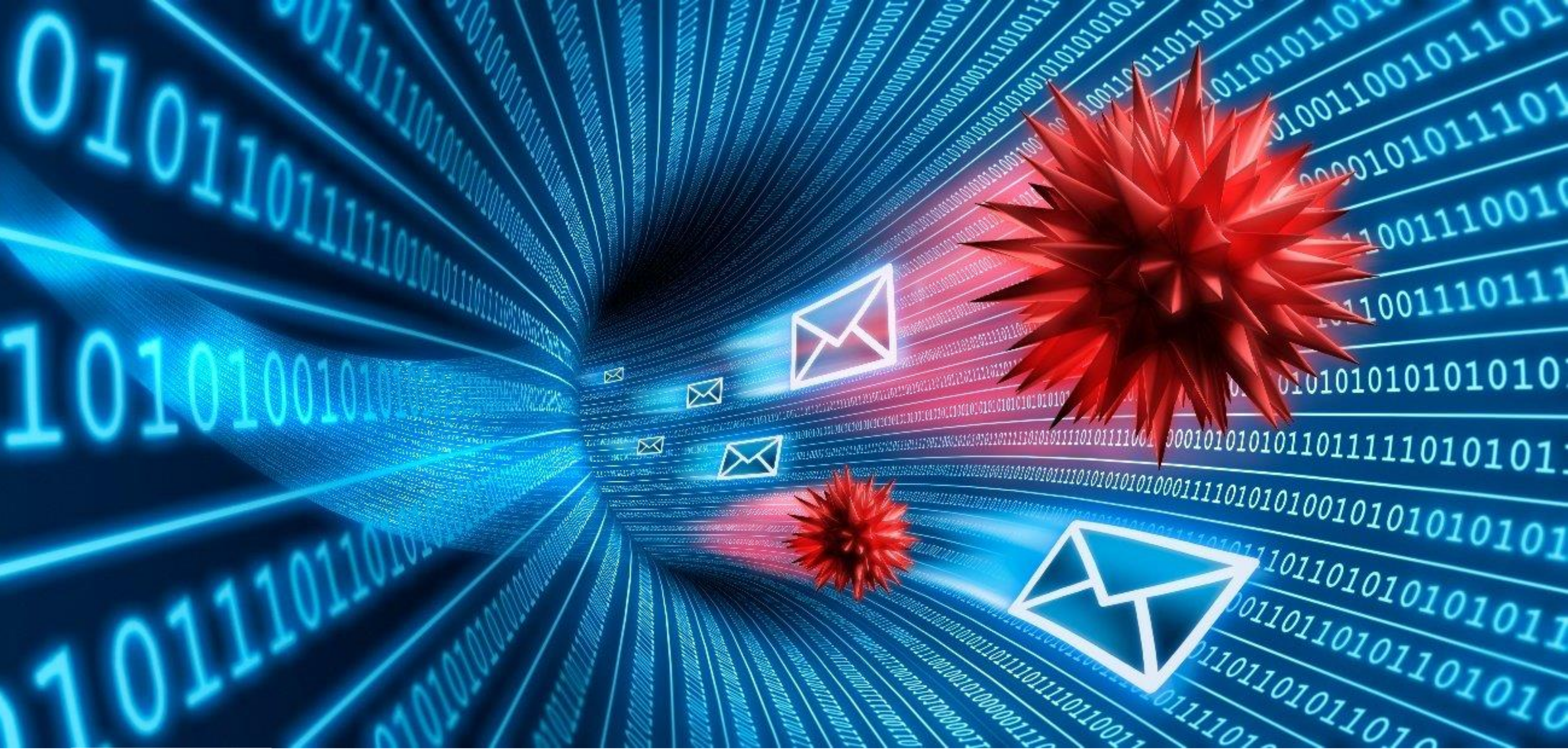
**TECHNOLOGY**
Are we leveraging the right Technology in the right way?



# Intuity Top Recommendations

1. **Training** your team can build a Human Firewall which will reduce the threat of attack
2. Keep your systems up-to-date: **Patching** operating systems, software, and firmware regularly
3. **Use multi-factor authentication** where possible
4. **Go to the Cloud** – securing your data and systems
5. Regularly change passwords and **avoid reusing passwords** for different accounts (use a password manager)
6. Audit user accounts with **administrative privileges** and configure access controls with "least privilege"
7. **Identify critical information assets** such as patient / customer database servers
8. Follow the **"3-2-1 Rule"** for backups
9. **Review Work from home arrangements**

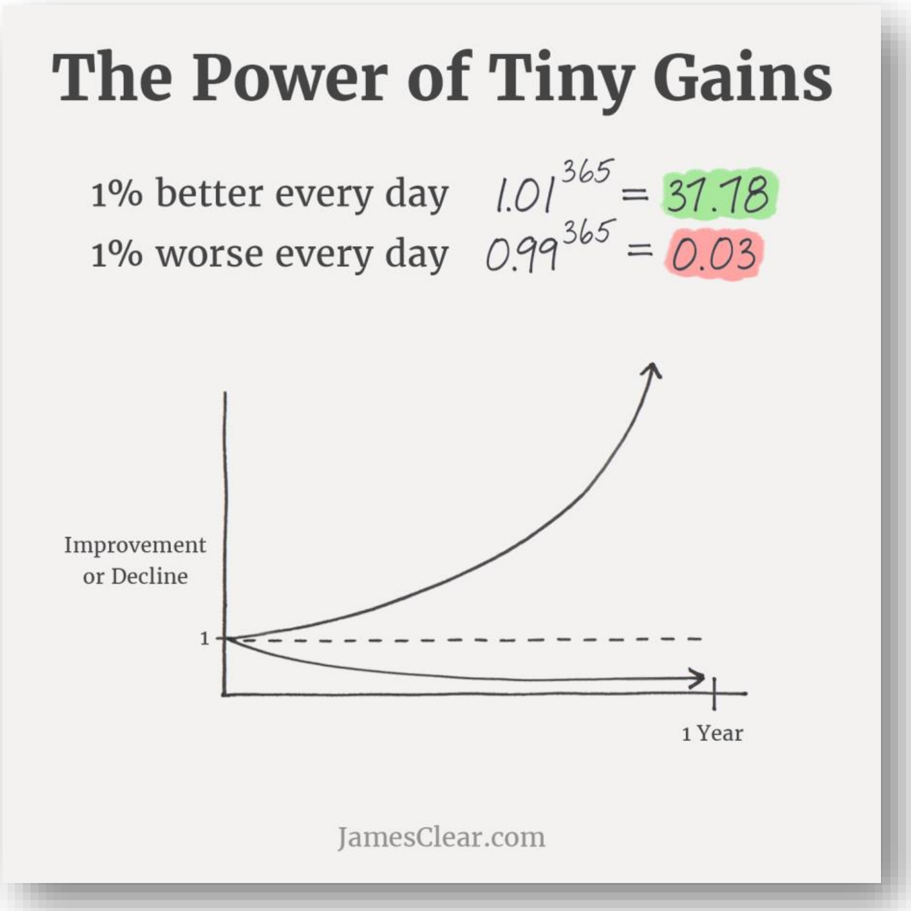
intuity



# Discussion, Q & A

MBA ASSOCIATION OF IRELAND

intuity



The Power of Tiny Gains

1% better every day $1.01^{365} = 37.78$

1% worse every day $0.99^{365} = 0.03$

JamesClear.com

# What Next?

- Apply a multi-layered approach
- Training & Culture of Awareness
- Apply a simple Framework
- Talk to us – we'd be delighted to help

- https://www.intuity.ie/connect/subscribe/
- hello@intuity.ie

# Notes & Resources

- Notes
- Resources
- Links
- Recommended reading / listening
- Framework information

# Our Top Recommendations (with some extra notes)

## Training & Phishing Simulation

- Training your team can build a Human Firewall which will reduce the threat of attack and increase your protection
- Phishing Simulation to raise user awareness and create a powerful Culture

## Keep your systems up-to-date:

- Patch operating systems, software, and firmware regularly

## Use multi-factor authentication where possible

## Regularly change all passwords

- Avoid reusing passwords for different accounts (use a password manager)

## Audit user accounts with administrative privileges

- Configure access controls with "least privilege" in mind

## Identify critical information assets

- Such as patient / customer database servers; create backups of these systems and house the backups offline from the network

## Follow the "3-2-1 Rule" for backups

- 3 copies of data (Live, Backup 1, Backup 2)
- 2 distinct backup types (e.g. local & cloud)
- 1 offsite copy (i.e. cloud)

## Review Work from home arrangements

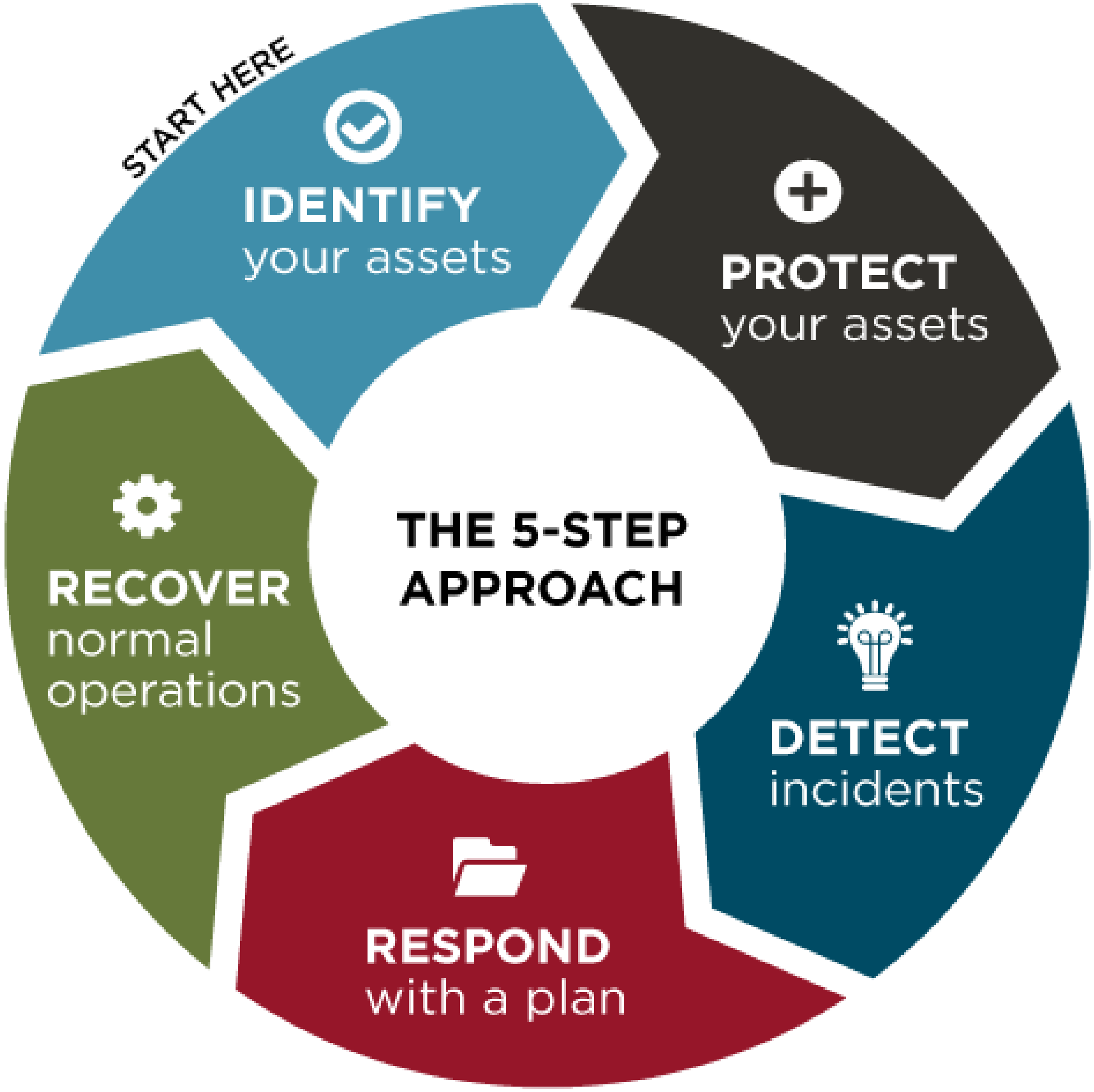
# Use a recognised framework for guidance

ISO 27001 CERTIFICATION EUROPE™

COBIT® 5 AN ISACA® FRAMEWORK

NIST

CYBER ESSENTIALS



NIST

# Framework for Cyber Security

intuity

# Resources / Recommended Media

- Books
  - “Zucked” – Roger McNamee
  - “The Dark Web” & “The People vs. Technology” – Jamie Bartlett
  - “Atomic Habits” – James Clear
- Podcasts
  - Darknet Diaries, Hacking Humans, Smashing Security

- Teams – Working from home! https://www.youtube.com/watch?v=-wCyq9oll_o
- Web
  - Cyber Essentials https://www.intuity.ie/data-it-security/cyber-essentials/
  - Dark Reading www.darkreading.com : Connecting The Information Security Community
  - Cyber Ireland https://cyberireland.ie/
  - Microsoft Report – Securing the Future, The Cyber Security Climate in Ireland. https://info.microsoft.com/rs/157-GQE-382/images/EN-CNTNT-eBook-Securingthefuture-MGC0003544.pdf

- More on NIST
  - https://www.nist.gov/cyberframework/online-learning/five-functions
  - https://www.secmatters.com/blog/how-to-comply-with-the-5-functions-of-the-nist-cybersecurity-framework

# NIST Framework for Cyber Security

## IDENTIFY

- Asset Management
- Business Environment
- Governance
- Risk Assessment
- Risk Management Strategy

## PROTECT

- Access Control
- Awareness & Training
- Data Security
- Info Protection Process & Procedures
- Maintenance
- Protective Technology

## DETECT

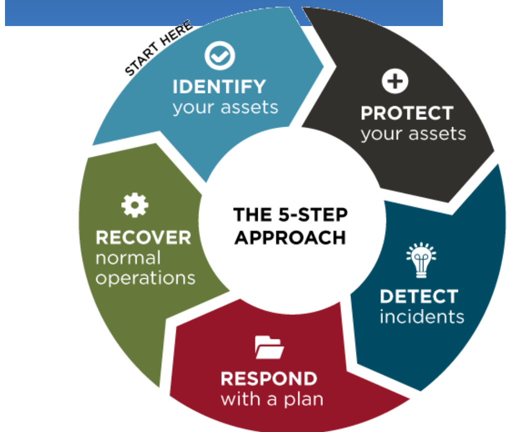
- Anomalies & Events
- Security & Continuous Monitoring
- Detection Processes

## RESPOND

- Response Planning
- Communications
- Analysis
- Mitigation
- Improvements

## RECOVER

- Recovery Planning
- Improvements
- Communications



# Posters / graphics for increasing awareness

When you leave your desk please...

Key + L

Lock your workstation

If a colleague forgets to do this please remind them

Passwords are like underwear...

⚠ Change them regularly

⚠ Dont share them with strangers

⚠ Dont leave them lying around

All passwords should be stored & encrypted in **Password Safe**

ISO 27001 CERTIFICATION EUROPE ™

intuity