

Creative Content Plan

Q2

In consultation with our customer base, we're pleased to launch our Q2 Creative Content Plan. The content is focussed on addressing the most pressing risks to your users, from the continually evolving risks posed by **Artificial Intelligence**, to refresher content on the **Core Cyber** risks. There is additional content to help remediate the **unique threats** faced by specific user bases, and the exponential rise in **Operational Technology cyber attacks**.



Creative Content Plan - Q2

Artificial Intelligence

Artificial Intelligence, or AI, is the greatest technological change since the invention of the internet. And with the many advantages it offers to productivity and efficiency, it also comes with its own **set of risks**.

These AI titles help employees understand the evolving threat of more sophisticated spear phishing attacks, which are being experienced by a wider range of staff. The content also helps learners understand the different types of AI tools, and why some are best suited to specific tasks.

Benefits of the Content:

- **Enhance your organisational resilience** against sophisticated AI-driven threats.
- Provide your teams with critical insights to **identify and mitigate AI-related risks**.

AI Series

AI: The Right Tool for the Right Job

Learn the difference between Generative and Summary AI, and the type of task each is best suited to.



Risk covered: **Artificial Intelligence**



Localised in 17 core languages and 26 additional subtitles.
Available from **30/09/2024**

AI: Can You Really "Do it Yourself"?

Learn how internal AI systems can rival proprietary AI, and even provide enhanced data protection and increased accuracy at a low cost.



Risk covered: **Data Protection**



Localised in 17 core languages and 26 additional subtitles.
Available from **30/09/2024**

Predicting the Next Word: How AI LLMs Work

Learn how Large Language Models are used by AI systems to generate complex answers that traditional software struggles with.



Risk covered: **Artificial Intelligence**



Localised in 17 core languages and 26 additional subtitles.
Available from **30/09/2024**

AI and Phishing: The Sophisticated Approach

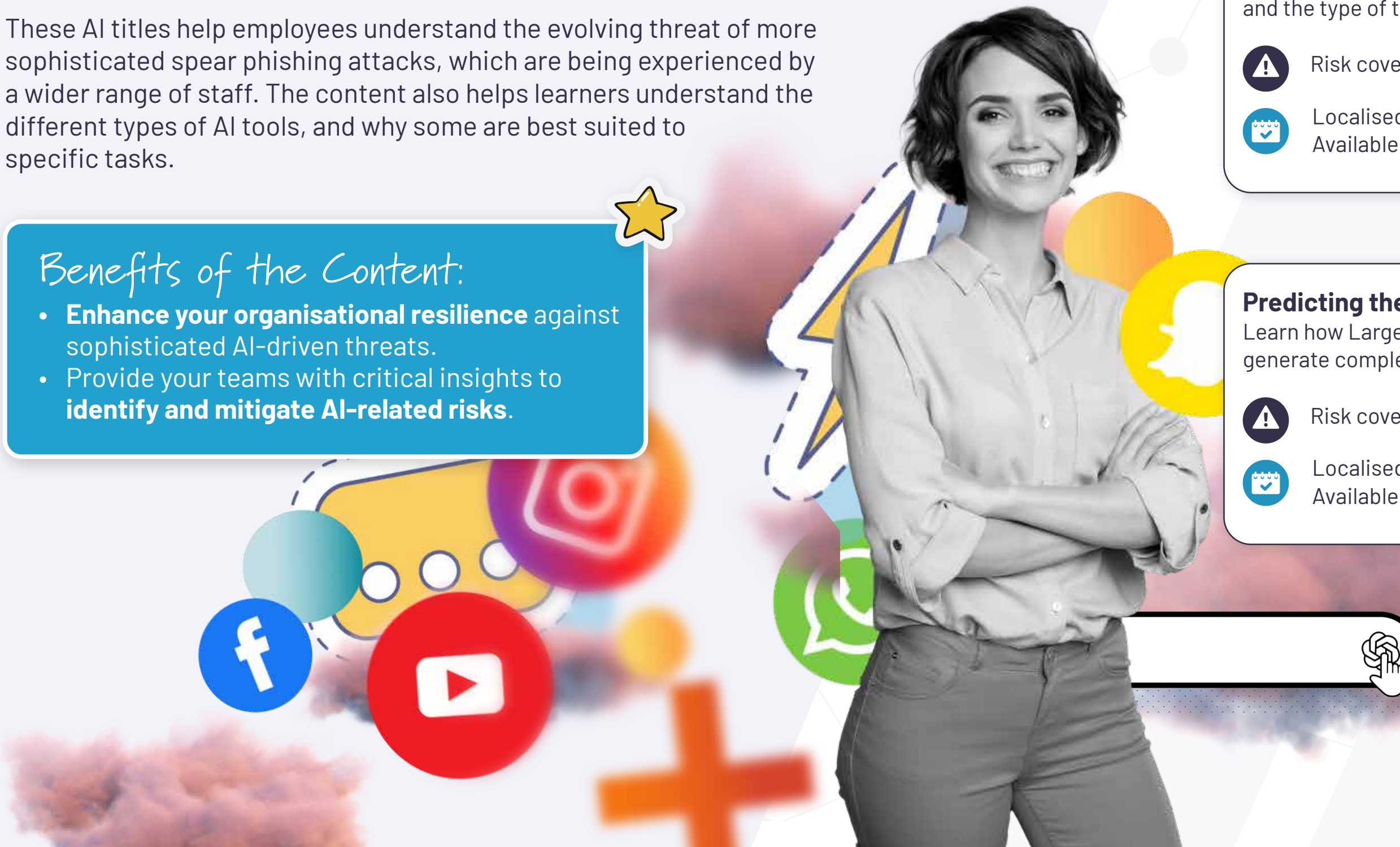
Learn how cyber criminals harvest information from online sources and use AI systems to create increasingly sophisticated phishing attacks.



Risk covered: **Phishing**



Localised in 17 core languages and 26 additional subtitles.
Available from **30/09/2024**





Creative Content Plan - Q2

Core Cyber Refresh


While common cyber attacks continue to evolve, employees still require regular updates on the core threats they face to improve their cyber awareness posture.

With refresher content in the ongoing "Essentials" series, the more advanced "Essentials Plus" program, short format content in the "Cyber in 60" titles, and the expansion of interactive content, there is a wide range of content to drive behaviour changes and reduce the human risk factor.

Securing your Mobile Phone - The Essentials


Learn how to keep your mobile phone secure from cyber criminals attempting to steal data.

 Risk covered: **Mobile Devices**

 Localised in 17 core languages and 26 additional subtitles.
Available from **26/08/2024**

Hybrid Working - The Essentials

Recognise that by practicing basic principles of data protection, we can help keep our sensitive data safe in all modes of working.

 Risk covered: **Information Security**

 Localised in 17 core languages and 26 additional subtitles.
Available from **30/09/2024**

The Essentials Plus

Email Security - Essentials Plus

Learn how to protect yourself and your organisation by only using email for work purposes, confirming the recipients, and protecting attachments.

 Risk covered: **Email**

 Localised in 17 core languages and 26 additional subtitles.
Available from **30/09/2024**

Remote Working - Essentials Plus

Learn why working remotely can place your devices and data in danger of loss or theft.

 Risk covered: **Mobile Devices**

 Localised in 17 core languages and 26 additional subtitles.
Available from **30/09/2024**

Password Security - Essentials Plus

Learn how to protect your accounts with a strong password and how MFA can add an additional layer of security.

 Risk covered: **Passwords**

 Localised in 17 core languages and 26 additional subtitles.
Available from **30/09/2024**

Data Handling - Essentials Plus

Learn how to protect sensitive data throughout its lifecycle by understanding and implementing best practices for data handling and responding effectively to data breaches.

 Risk covered: **Information Security**

 Localised in 17 core languages and 26 additional subtitles.
Available from **30/09/2024**

Benefits of the Content:

- Maintain a **robust cyber security posture** across your organisation.
- Ensure your workforce is **continuously updated** on cyber security best practices.





Creative Content Plan - Q2

Core Cyber Refresh

Preventing Misdirected Email Breaches

Learn the difference between the CC and BCC email fields, and how to protect individuals' email addresses by using the BCC field.

Risk covered: **Email**

Localised in 22 core languages and 21 additional subtitles.
Available from **29/07/2024**

Cyber in 60

Maximise engagement and knowledge retention with content focussed on addressing one key risk in 60 seconds or less.



Phishing – Take 6

Learn why it is important to count to 6 when an email tries to scare you into taking action.

Risk covered: **Social Engineering**

Localised in 17 core languages and 26 additional subtitles.
Available from **30/09/2024**

HTTPS – Is it Safe?

Learn why HTTPS isn't a sign that a website can be trusted.

Risk covered: **Internet**

Localised in 17 core languages and 26 additional subtitles.
Available from **30/09/2024**

Interactivity

Access Control – What Would You Do?

Unauthorised access to an organisation can place sensitive data at risk of loss or theft. How would you respond to tailgating scenarios?

Risk covered: **Access Control**

Localised in 17 core languages and 26 additional subtitles.
Available from **30/09/2024**



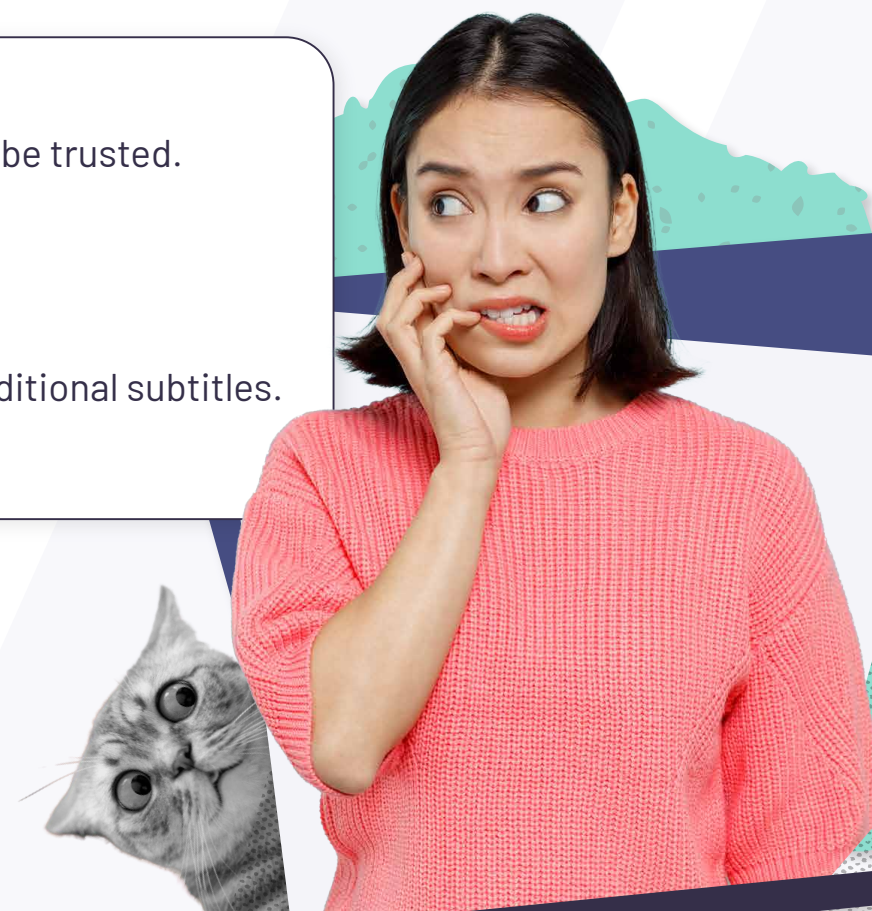
BCC: J.JONES@SAKZ.ORG,

To whom it may concern,

I am writing to apologise for sending an email on 21/6 as it was not intended for you.

As this information is private, you do not have the right to use any of the information it contains, and I would ask that you **delete this email immediately.**

Many thanks.





Creative Content Plan - Q2

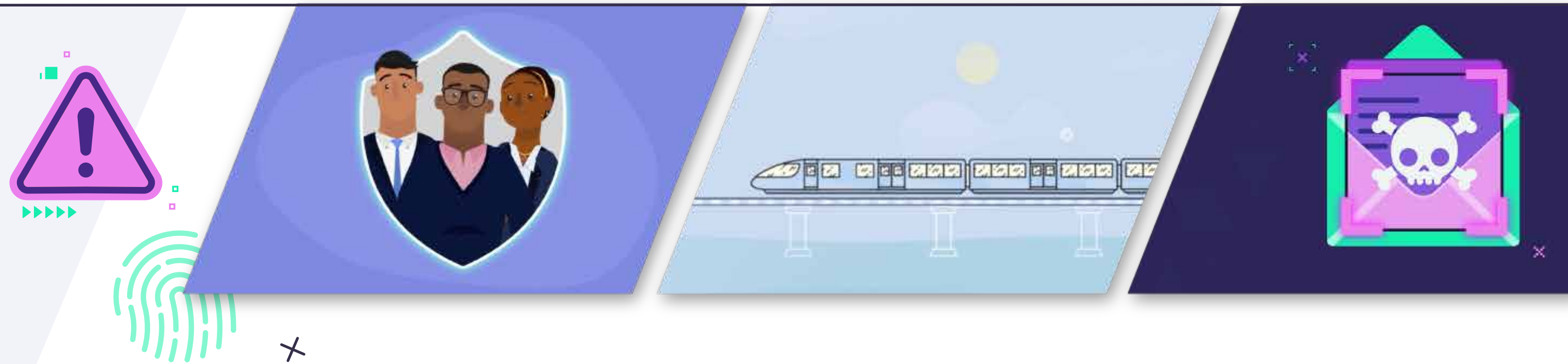
Departmental Series - Sales, Legal and Procurement

Cyber security messaging is most effective when it speaks to the audience's unique needs. The continuation of the series for Sales, Legal and Procurement departments speaks to these needs.

Every role experiences common threats in a unique way. Whether it's access control, shadow IT, the risks from social media and social engineering, or not properly following data classification rules, the attacks and consequences of a breach can be very different, depending on the access of the targeted individual.

Given their access to a wide range of information, and as they naturally deal with external partners and customers, Sales, Legal and Procurement staff are a prime target for cybercriminals.

This content will help your employees in these roles understand the unique challenges they face, and the remediation they can follow to protect both themselves, and the organisation.



6 Procurement Department nanos:

- ⚠ Localised in 17 core languages and 26 additional subtitles.
- 📅 Available from **29/07/2024**

- The Dangers of Tailgating
- The Dangers of Shadow IT
- The Dangers of Business Email Compromise
- The Dangers of Social Media
- The Dangers of Getting Hacked
- The Dangers of Unclassified Data

6 Legal Department nanos:

- ⚠ Localised in 17 core languages and 26 additional subtitles.
- 📅 Available from **26/08/2024**

- The Dangers of Tailgating
- The Dangers of Shadow IT
- The Dangers of Ransomware
- The Dangers of Social Engineering
- The Dangers of Getting Hacked
- The Dangers of Unclassified Data

6 Sales Department nanos:

- ⚠ Localised in 17 core languages and 26 additional subtitles.
- 📅 Available from **26/08/2024**

- The Dangers of Tailgating
- The Dangers of Shadow IT
- The Dangers of Malicious Software
- The Dangers of Social Engineering
- The Dangers of Getting Hacked
- The Dangers of Unclassified Data

Benefits of the Content:

- Cyber security content **tailored to unique departmental risks**.
- **Minimise targeted cyber attacks** through role-specific content.



Creative Content Plan - Q2

Operational Technology

OT is facing increased cyber security risks. With diverse and often unique technical infrastructure, the evolution of the Industrial Internet of Things, and the increased focus of regulators and cybercriminals, the challenges are immense.

The first part of our OT content will help operators understand the threats they face, and how they can protect their organisation. With a broad introduction on the importance of Cyber Safety in OT environments, followed by specific content on the risk of USB devices, Password Security and how OT environments are coming under increasing Phishing and Social Engineering attacks, the initial content in the OT series helps operators understand the human risk factors in cyber security, and address some of the most common threats the industry faces.

Operational Technology Defence: Modern Cyber Safety Practices

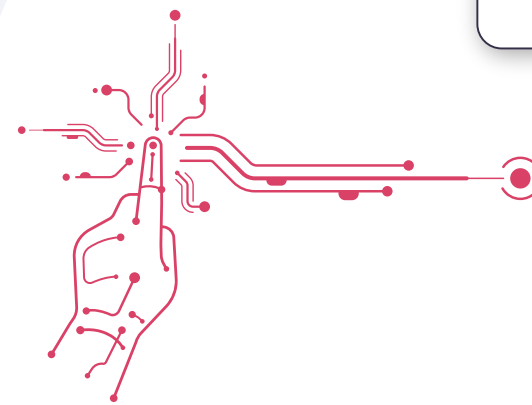
Learn how the USB devices, poor password hygiene and phishing pose a real risk to our Cyber Safety.

 Risk covered: **Multi-Vector**

 Localised in 17 core languages and 26 additional subtitles.
Available from **26/08/2024**

Benefits of the Content:

- Fortify your OT infrastructure against **escalating cyber security risks**.
- Address contemporary cyber security best practices to **protect critical infrastructure**.



Quishing (QR Code Jacking)

Would You Trust an MFA QR Code

Learn how criminals are using QR codes in Phishing emails, pretending to be MFA alerts.

 Risk covered: **Email**

 Localised in 17 core languages and 26 additional subtitles.
Available from **30/09/2024**



Multi Factor Authentication

What is MFA?

Learn what Multi-Factor Authentication is and how it can help you to protect your user accounts.

 Risk covered: **Passwords**

 Localised in 17 core languages and 26 additional subtitles.
Available from **30/09/2024**



Creative Content Plan - Q2

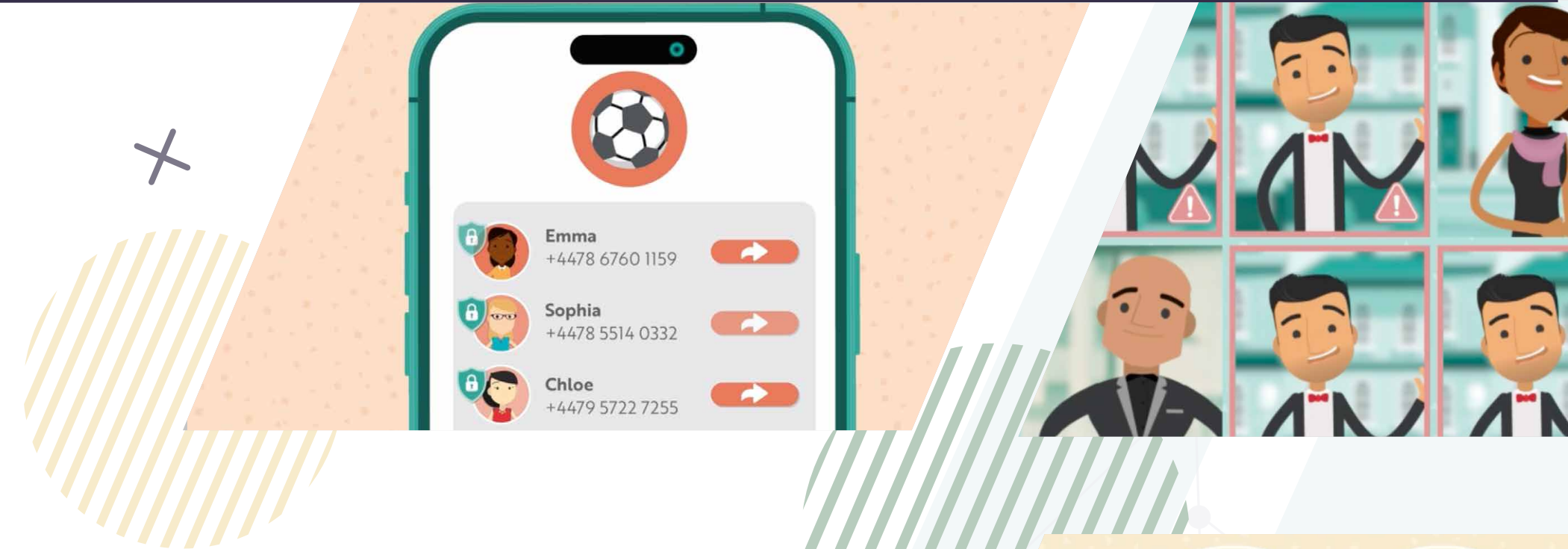
Student Series

Ongoing reports indicate that under 25s are at more likely to be the victims of cyber crime than any other group. Students face their own specific risks within this demographic.

To support Universities and Further Education institutes, these titles help students understand the personal cyber security and social engineering risks they face and how these can be identified and avoided.

Benefits of the Content:

- Cyber security awareness content **tailored to the unique risks students encounter.**
- Ensure the student population understands how **cyber attacks** will be **targeted** at them.



Student Cyber Security – Doxing

Discover the dangers to your personal information from doxing, and how you can avoid the risk.

- ⚠ Risk covered: **Information Security**
- 📅 Released in English only. Available from **30/09/2024**

Student Cyber Security – Smartphone Security

Discover how cybercriminals can exploit your mobile phone to steal personal and financial data, and steps you can take to help avoid this.

- ⚠ Risk covered: **Mobile Devices**
- 📅 Released in English only. Available from **30/09/2024**

Student Cyber Security – Safe Web Browsing

Learn how to keep your personal data safe while browsing online.

- ⚠ Risk covered: **Internet**
- 📅 Released in English only. Available from **30/09/2024**

Student Cyber Security – Avoiding Ransomware

Learn why ransomware attacks pose a serious risk to your academic life and discover how to safeguard your digital assets from cybercriminals.

- ⚠ Risk covered: **Malware**
- 📅 Released in English only. Available from **30/09/2024**

Student Cyber Security – Avoiding Harmful Content

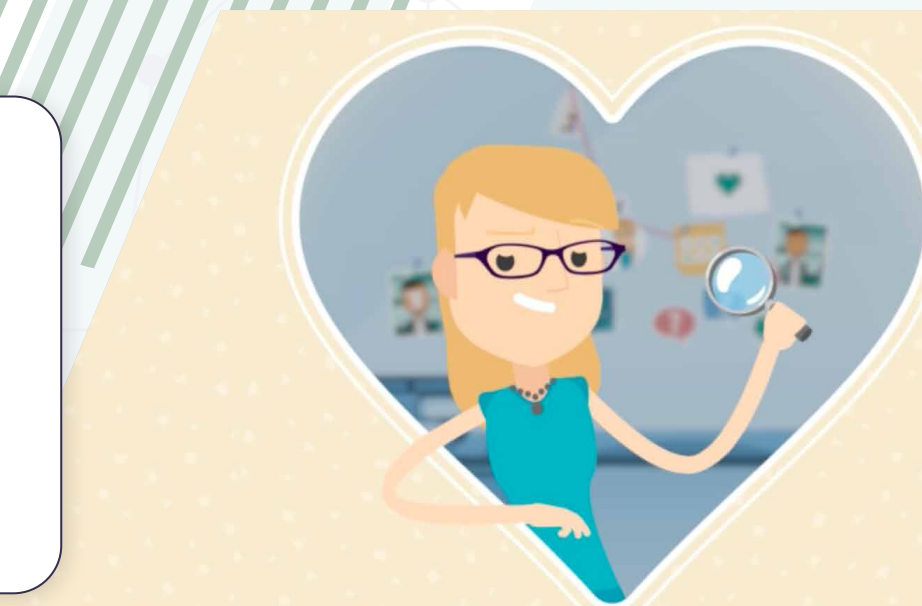
Recognise red flags like encouragement to break the law, coded language, fact-checking warnings, requests to move conversations to private channels, and report suspicious content.

- ⚠ Risk covered: **Personal Cyber Security**
- 📅 Released in English only. Available from **30/09/2024**

Student Cyber Security – Know Your Data

Exposure to cybersecurity threats such as identity theft, academic fraud, or financial loss can have severe consequences for students.

- ⚠ Risk covered: **Data Classification**
- 📅 Released in English only. Available from **30/09/2024**





Creative Content Plan - Q2

Phish and complementary Red Flags Learning Experiences

Throughout Q2, we will be releasing THREE new phish templates. Each template comes with a complementary Red Flags PDF Learning Experience, in 44 languages.

