



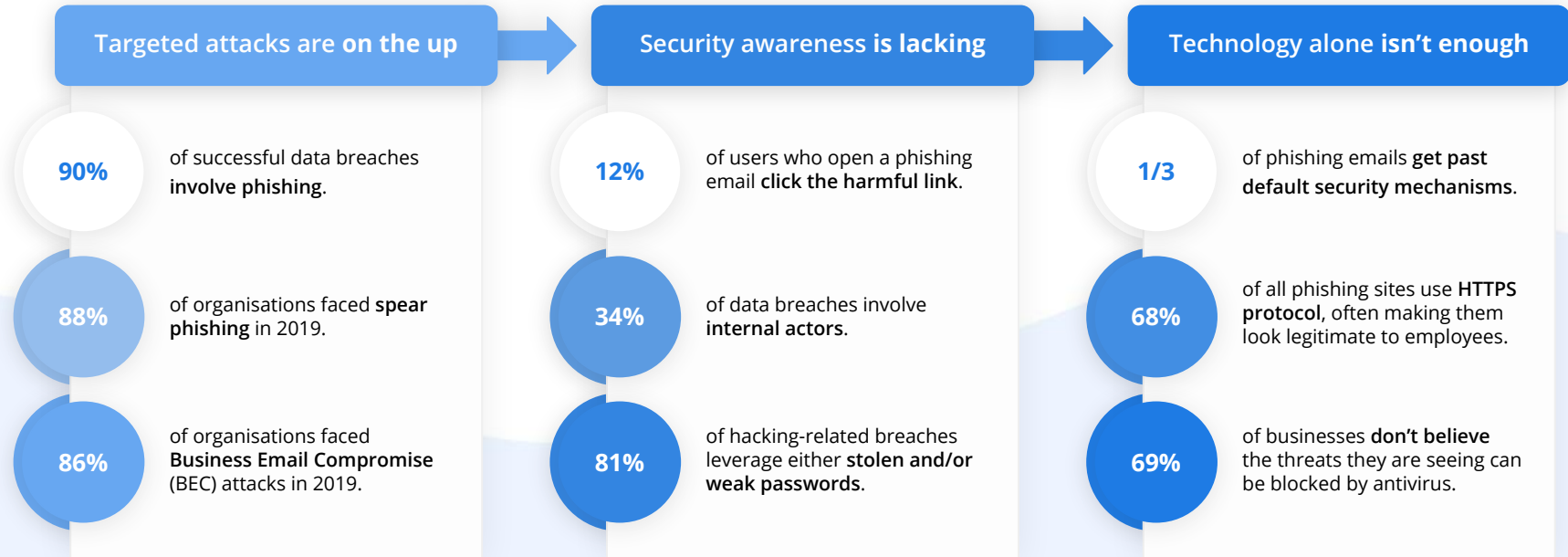
Cyber Awareness Training

VALUE PROPOSITION

Technology alone isn't enough to safeguard your business

Even with top-of-the-range endpoint protection, **cyber criminals will find intelligent ways of getting through the cracks.**

When they do, they'll use sophisticated social engineering techniques to **manipulate your employees** into giving away sensitive information.

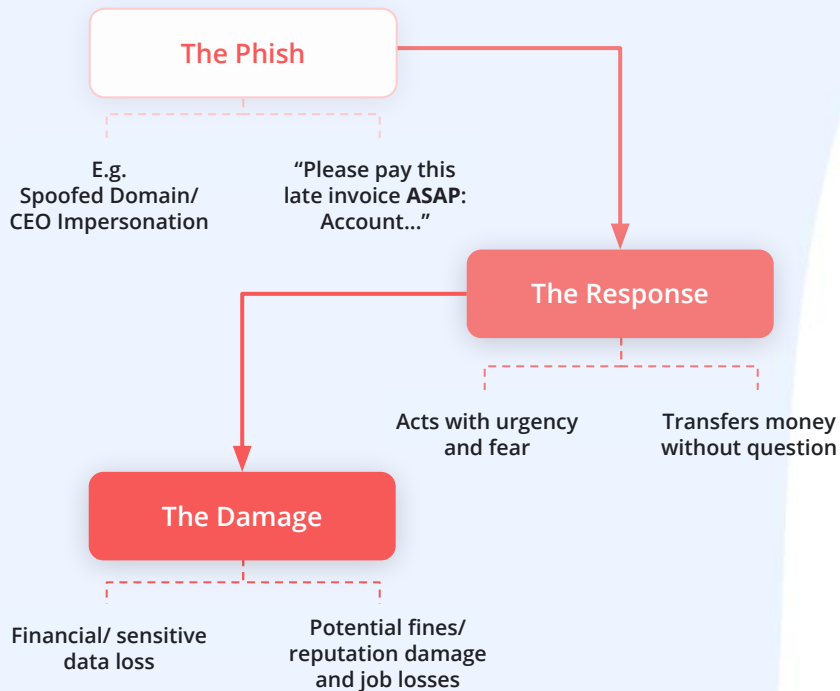


What are the potential risks to your business?

- Regulatory fines
- Financial loss
- Downtime and remediation
- Loss of corporate/ client data
- Decline in productivity
- Damage to company reputation

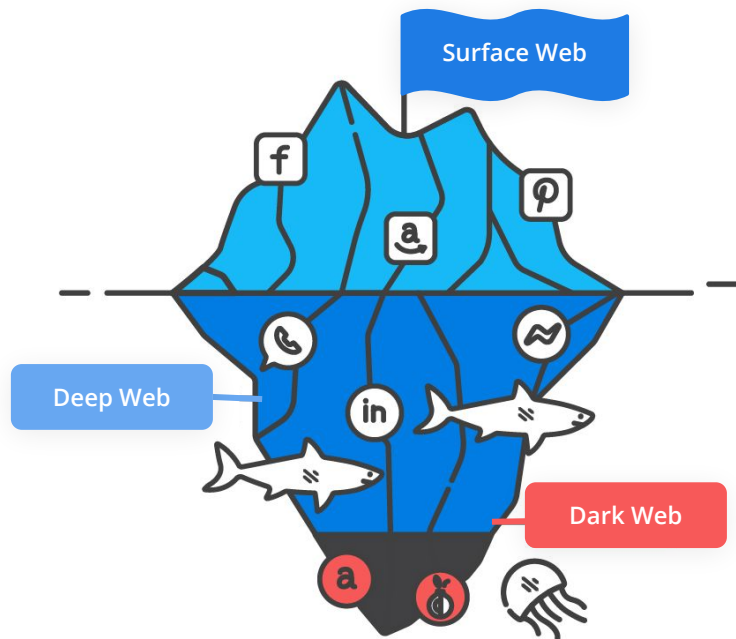
Phishing and social engineering are still the no.1 weapon of choice

Exploiting and manipulating users through phishing attacks is still the **no.1 attack vector** for cyber criminals.



Exposed data on the dark web is the go-to ammunition

With billions of sensitive data records exposed on the dark web - incl. active usernames, passwords and PII - cyber criminals can **gather all of the necessary resources** needed to pull off a successful attack.



Your employees aren't your weakest link - they're your **first line of defence** against cyber crime.

A lack of regular security awareness training, up-to-date communications and virtually no way of tracking user behaviour is often the main cause of employees falling victim to attacks.

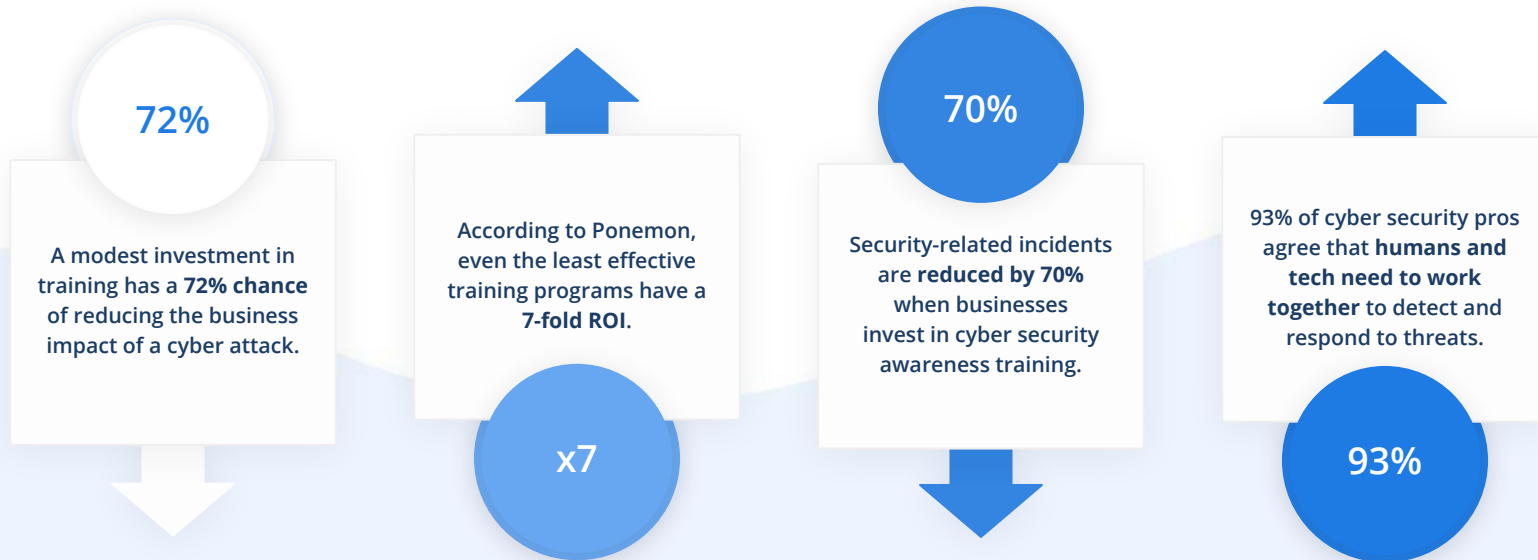
With an **effective security awareness training solution**, you can transform your users into a solid first line of defence for identifying, avoiding and reporting sophisticated attacks.



Train your employees to combat cyber threats and drive secure behaviour

Implement a **proactive approach to reducing employee cyber risk** by delivering effective computer-based security awareness training.

Train your users on key threats like phishing, social engineering and password hygiene, while simulating mock-phishing exercises that analyse employee vulnerability to targeted attacks.

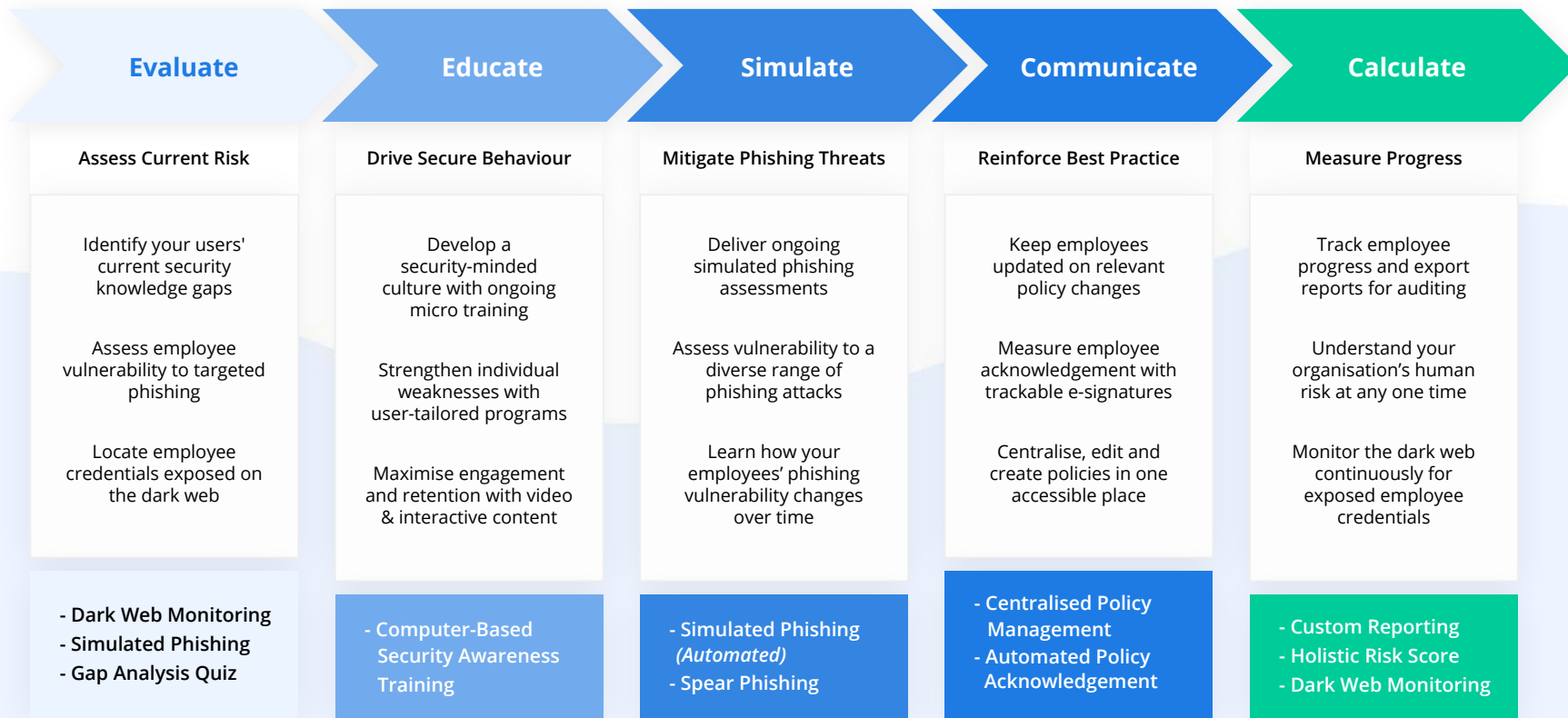


What are the main benefits for your business?

- ✓ Build a security-minded culture
- ✓ Reduce user-related incidents
- ✓ Avoid regulatory fines
- ✓ Achieve compliance
- ✓ Reduce downtime/ remediation
- ✓ Safeguard corporate/ client data

Here's how we transform your employees into a cyber security asset

We ensure **ongoing, bite-sized training** that strengthens your users' knowledge in core areas of security, while **measuring your organisation's overall human risk** based on continual phishing assessments, dark web monitoring and policy communications.



Get started today with a free **Employee Risk Assessment (ERA)**

Your free ERA report **identifies your employees' current risk level** to internal and external threats through calculating reality-based metrics, including;

- Your employees' current susceptibility to targeted phishing attacks
- What employee data is currently stolen/ exposed on the dark web

Internal Risk Assessment

We'll simulate a targeted spear phishing attack that closely replicates the techniques used by real world criminals.

External Risk Assessment

We'll identify your employees' compromised and stolen data that is exposed on the dark web and accessible to attackers.

Employee Risk Report

Your ERA report will outline the opened, clicked and compromised rates of your phishing test, as well as a breakdown of what user data is exposed on the dark web and which breaches they were exposed in.



If you would like to speak to a member of our team about this vital business service then please call **(01) 8424114** or email us at **hello@it.ie** and we'll get right back to you.