cymplify

People + Process

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.

cymplify

Targeted attacks are on the up

90% of successful data breaches **involve phishing**.

88% of organisations faced **spear phishing** in 2022

86% of organisations faced **Business Email Compromise** (BEC) attacks in 2022.

Security awareness is lacking

12% of users who open a phishing email **click the harmful link**.

34% of data breaches involve **internal actors**.

81% of hacking-related breaches leverage either **stolen and/or weak passwords**.

Technology alone isn't enough

1/3 of phishing emails **get past default security mechanisms**.

68% of all phishing sites use **HTTPS protocol**, often making them look legitimate to employees.

69% of businesses **don't believe** the threats they are seeing can be blocked by antivirus.

What are the potential risks to your business?

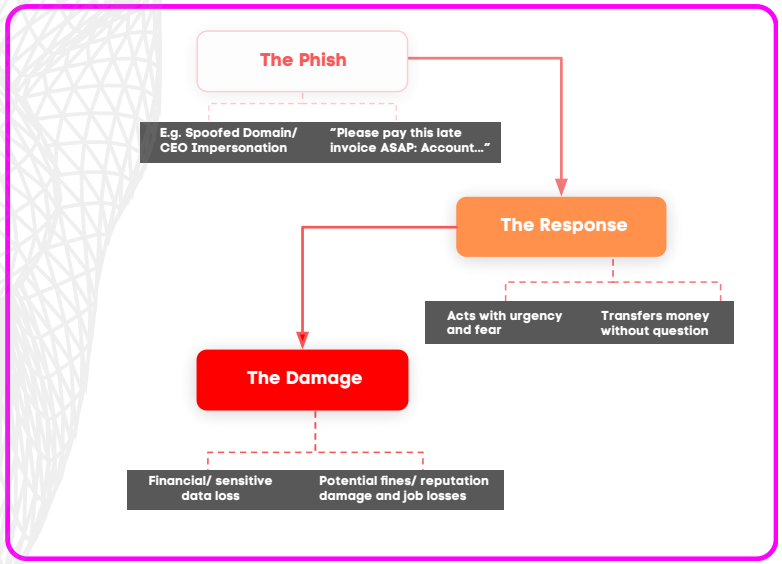
- **Regulatory fines**
- **Financial loss**
- **Downtime and remediation**
- **Loss of corporate/ client data**
- **Decline in productivity**
- **Damage to company reputation**

Data taken from Varonis, Verizon and Ponemon

cymplify

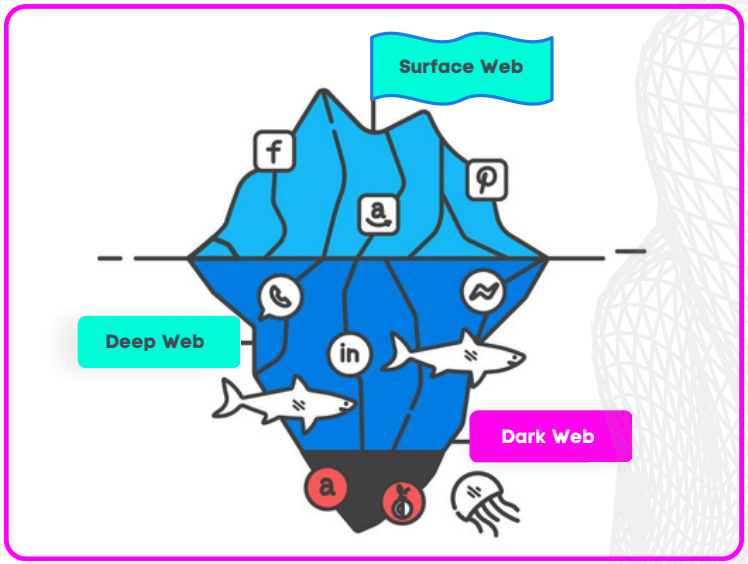
Phishing and social engineering are still the no.1 weapon of choice

Exploiting and manipulating users through phishing attacks is still the **no.1 attack vector** for cyber criminals - and this is set to get exponentially more serious with the advent of **generative AI**.



Exposed credential 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.



cymplify

Train your People 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.

72%

A modest investment in training has a 72% chance of reducing the business impact of a cyber attack.

According to Ponemon, even the least effective training programs have a 7-fold ROI.

x7

70%

Security-related incidents are reduced by 70% when businesses invest in cyber security awareness training.

93% of cyber security pros agree that humans and tech need to work together to detect and respond to threats.

93%

What are the main benefits for your business?

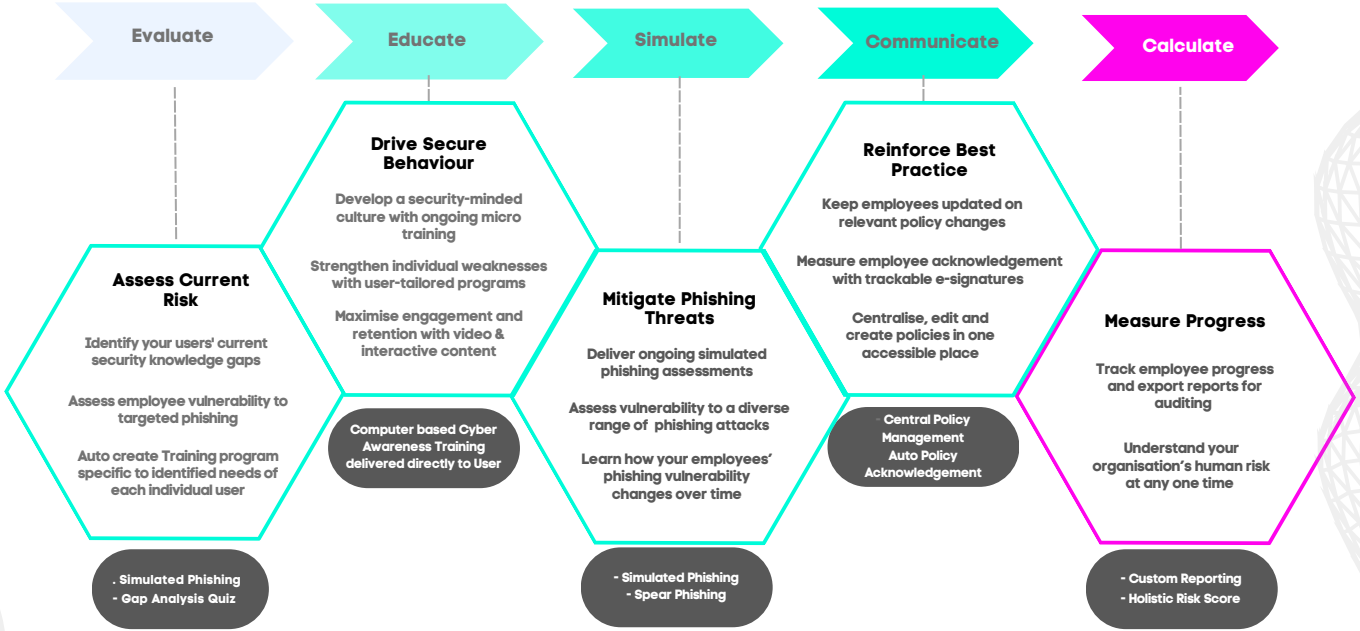
- ✓ Build a security-minded culture
- ✓ Reduce user-related incidents
- ✓ Avoid regulatory fines
- ✓ Achieve compliance
- ✓ Reduce downtime/ remediation
- ✓ Safeguard corporate/ client data

Data taken from Varonis, Verizon and Ponemon

cymplify

Here's how we transform your people into cyber risk assets

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 and policy communications.

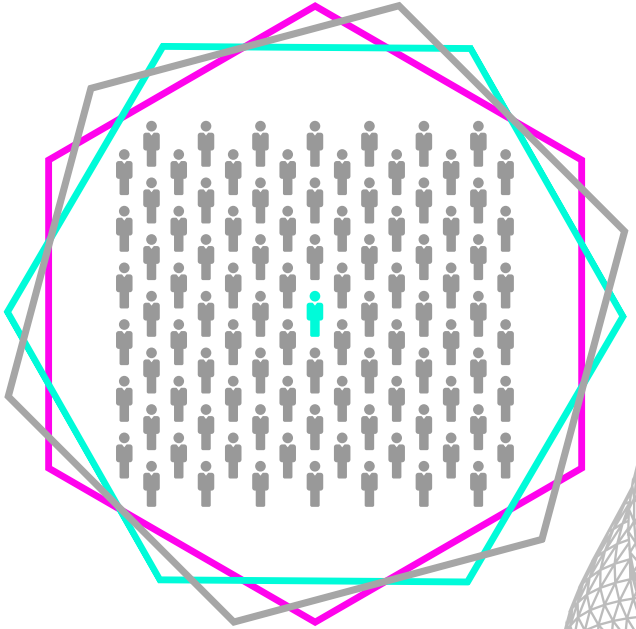


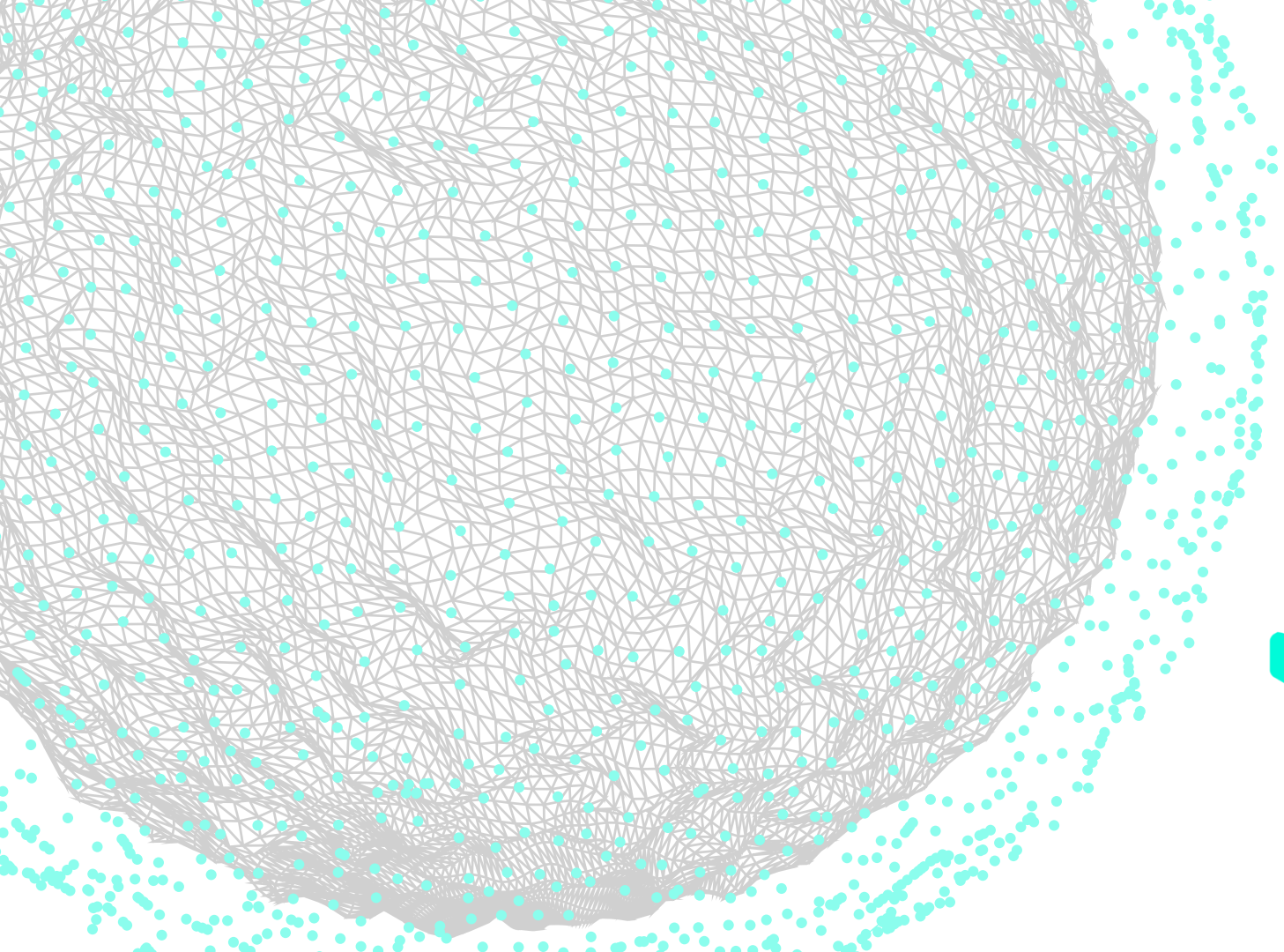
cymplify

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

A **lack of regular security awareness training**, no up-to-date communications and no usable way of tracking user behaviour are often the main causes of employees falling victim to attacks.

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





cymplify

w: www.cymplify.co.uk
e: hello@cymplify.co.uk
t: +44 (0)203 916 5121
@: 71 Shelton St,
London, WC2H 9JQ