info@itblue.co.za | www.itblue.co.za

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.

Targeted attacks are **on the up**

- **90%** of successful data breaches **involve phishing**.
- **88%** of organisations faced **spear phishing** in 2019.
- **86%** of organisations faced **Business Email Compromise** (BEC) attacks in 2019.

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?

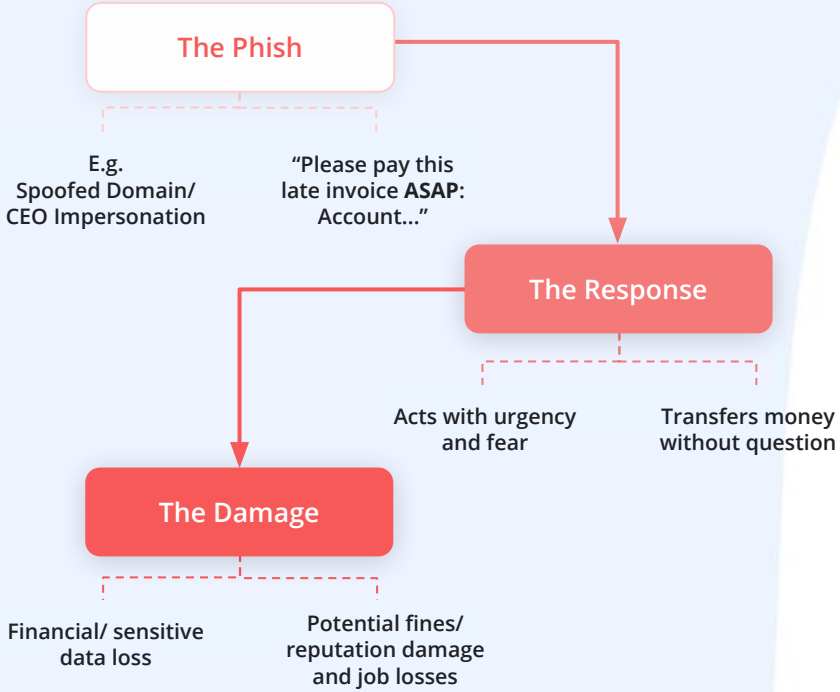
- **Regulatory fines**
- **Loss of corporate/ client data**
- **Financial loss**
- **Decline in productivity**
- **Downtime and remediation**
- **Damage to company reputation**

Data taken from Varonis, Verizon and Ponemon

info@itblue.co.za | www.itblue.co.za

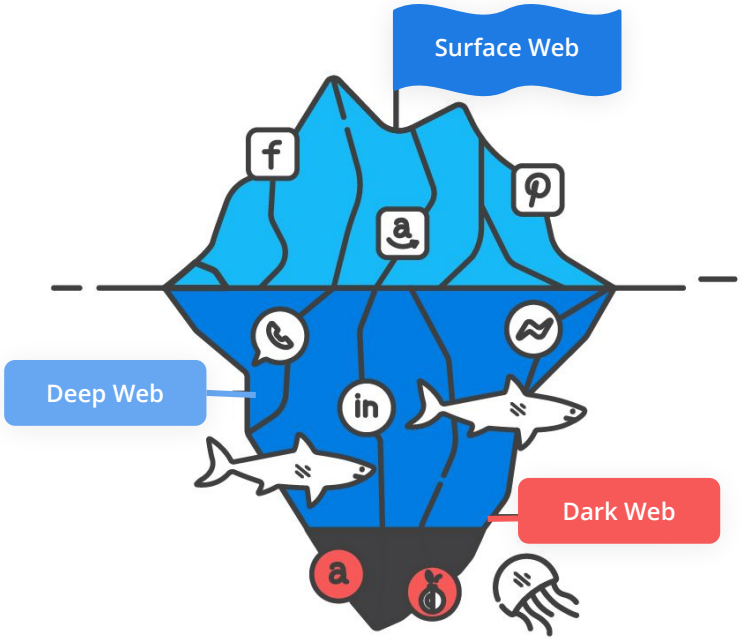
Phishing and social engineering are still the **no.1 weapon of choice**

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.

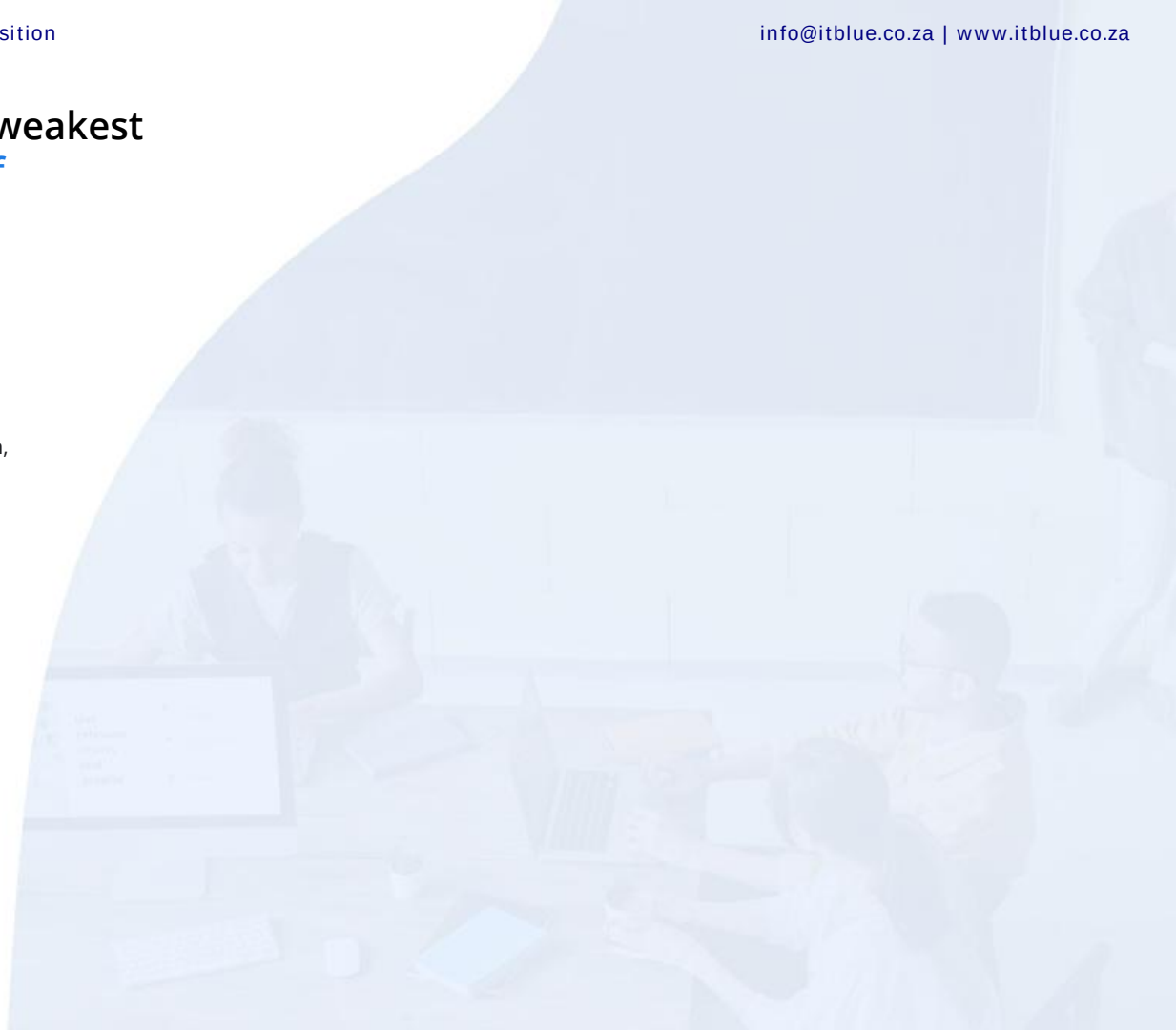


info@itblue.co.za | www.itblue.co.za

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.



info@itblue.co.za | www.itblue.co.za

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.

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

info@itblue.co.za | www.itblue.co.za

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.

Evaluate

Assess Current Risk

Identify your users' current security knowledge gaps

Assess employee vulnerability to targeted phishing

Locate employee credentials exposed on the dark web

- Dark Web Monitoring
- Simulated Phishing
- Gap Analysis Quiz

Educate

Drive Secure Behaviour

Develop a security-minded culture with ongoing micro training

Strengthen individual weaknesses with user-tailored programs

Maximise engagement and retention with video & interactive content

- Computer-Based Security Awareness Training

Simulate

Mitigate Phishing Threats

Deliver ongoing simulated phishing assessments

Assess vulnerability to a diverse range of phishing attacks

Learn how your employees' phishing vulnerability changes over time

- Simulated Phishing *(Automated)*
- Spear Phishing

Communicate

Reinforce Best Practice

Keep employees updated on relevant policy changes

Measure employee acknowledgement with trackable e-signatures

Centralise, edit and create policies in one accessible place

- Centralised Policy Management
- Automated Policy Acknowledgement

Calculate

Measure Progress

Track employee progress and export reports for auditing

Understand your organisation's human risk at any one time

Monitor the dark web continuously for exposed employee credentials

- Custom Reporting
- Holistic Risk Score
- Dark Web Monitoring

info@itblue.co.za | www.itblue.co.za

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**