



Introducing LevelUp e-Learning

THE CYBER SECURITY PLATFORM FOR YOUR STAFF



Presenter

Matias Garcia-Verdous

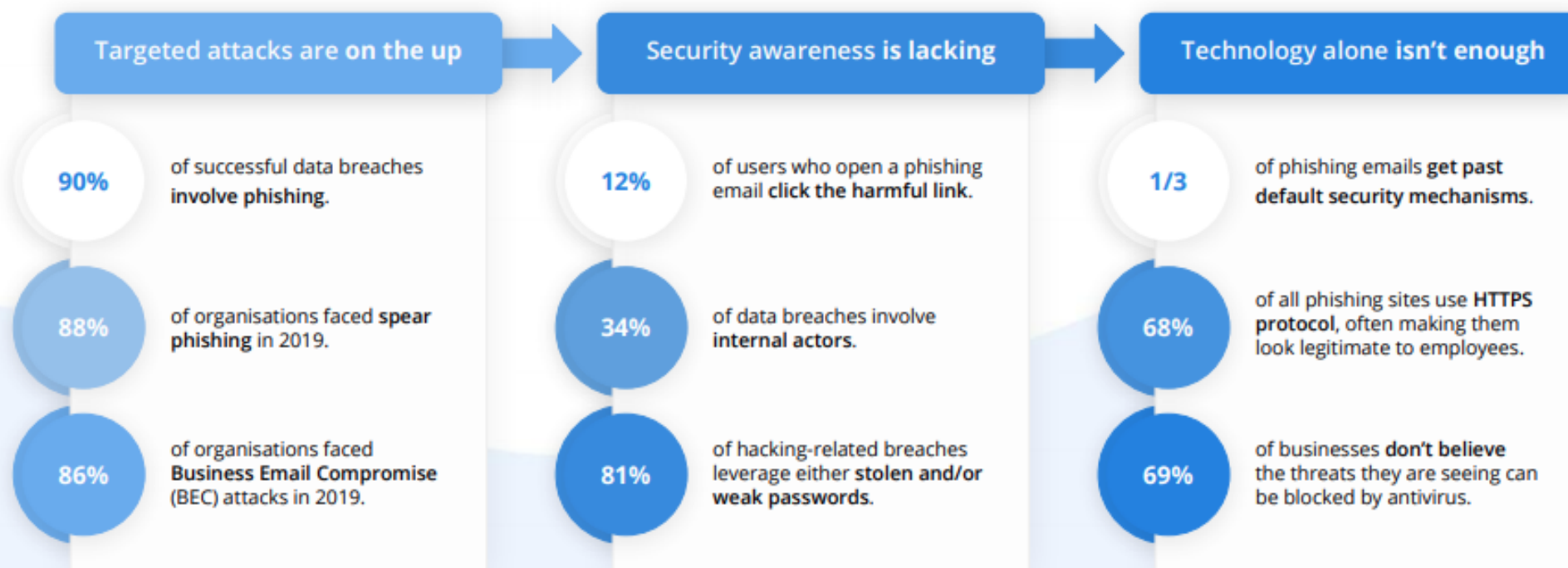


Technology alone isn't enough to safeguard your business

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

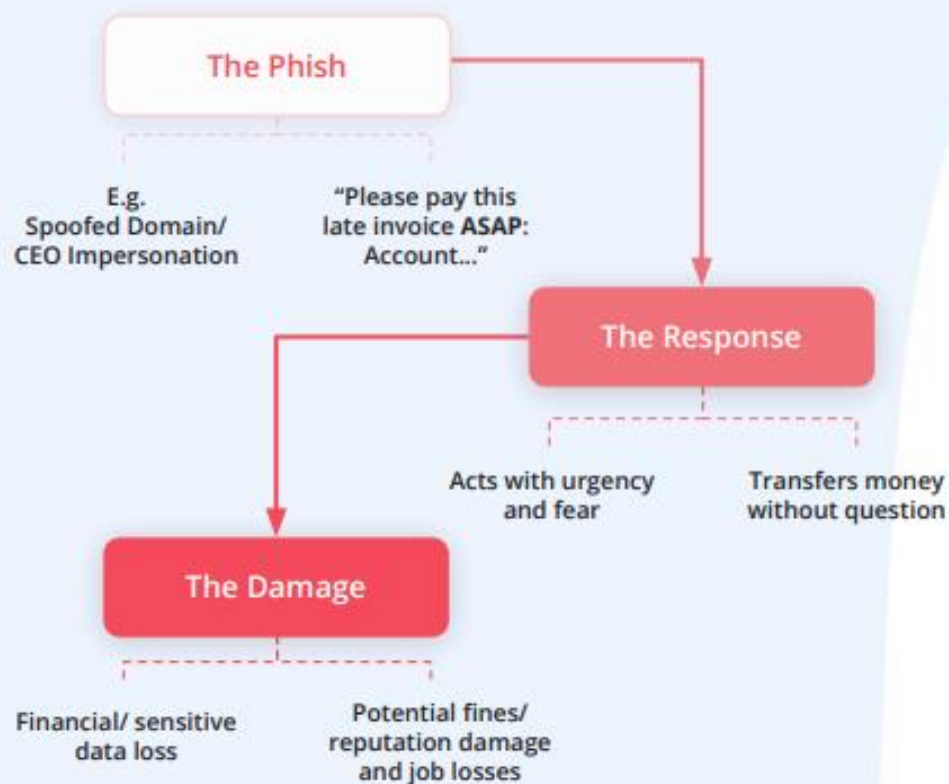
Data taken from Varonis, Verizon and Panemon



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

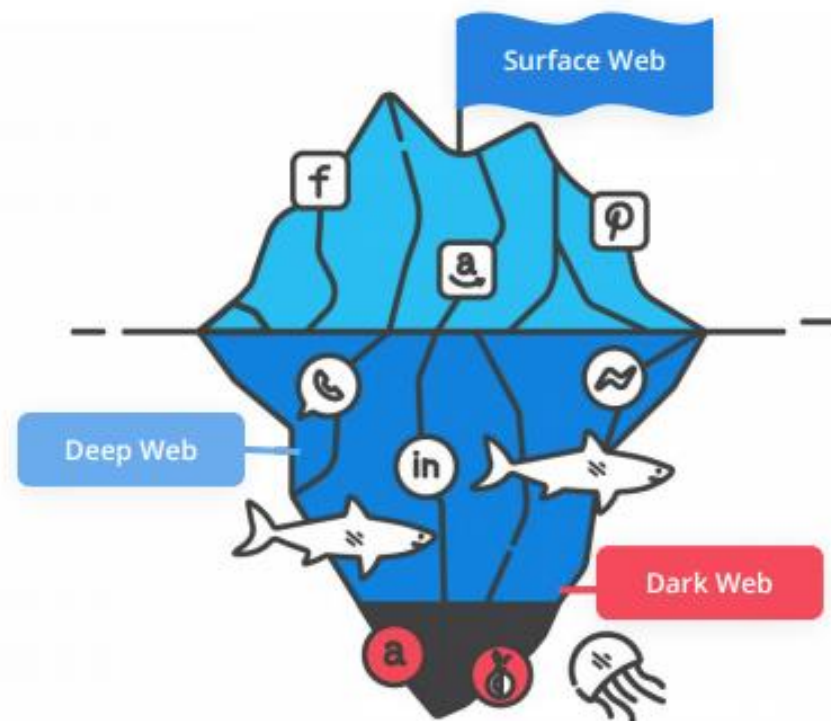
Phishing and social engineering are still the no.1 weapon of choice

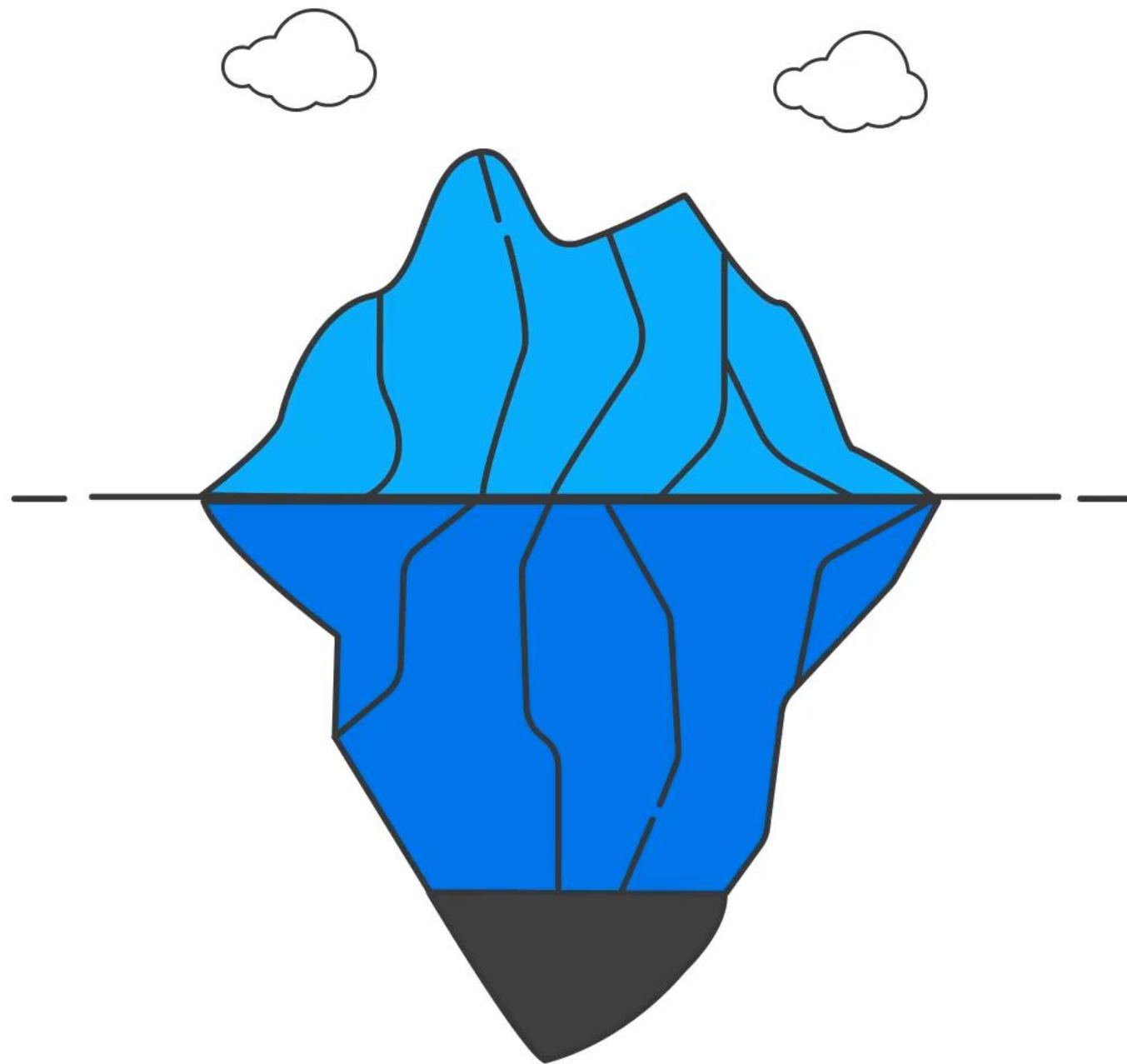
Exploiting and manipulating users through phishing attacks is still the **no.1 attack vector** for cyber criminals.



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.





Most of the Web is hidden.

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.



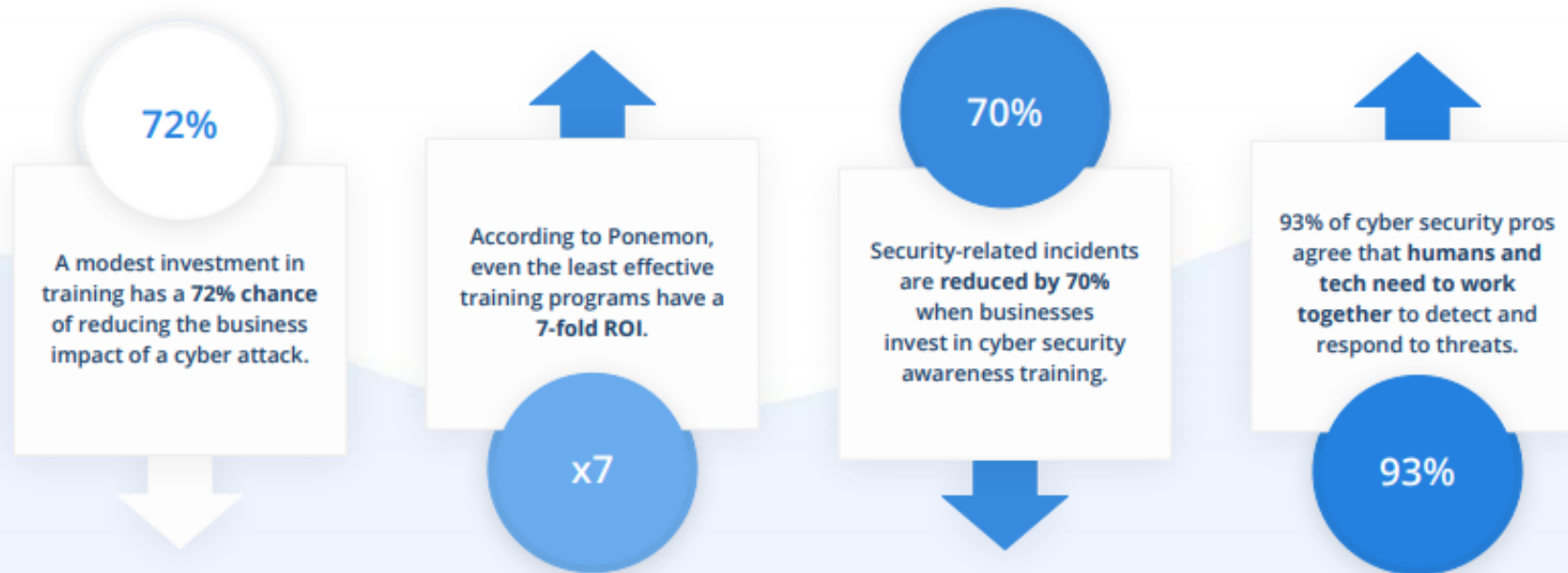


Train your employees to combat cyber threats and drive secure behaviour

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
- ✓ Avoid regulatory fines
- ✓ Reduce downtime/ remediation
- ✓ Reduce user-related incidents
- ✓ Achieve compliance
- ✓ Safeguard corporate/ client data

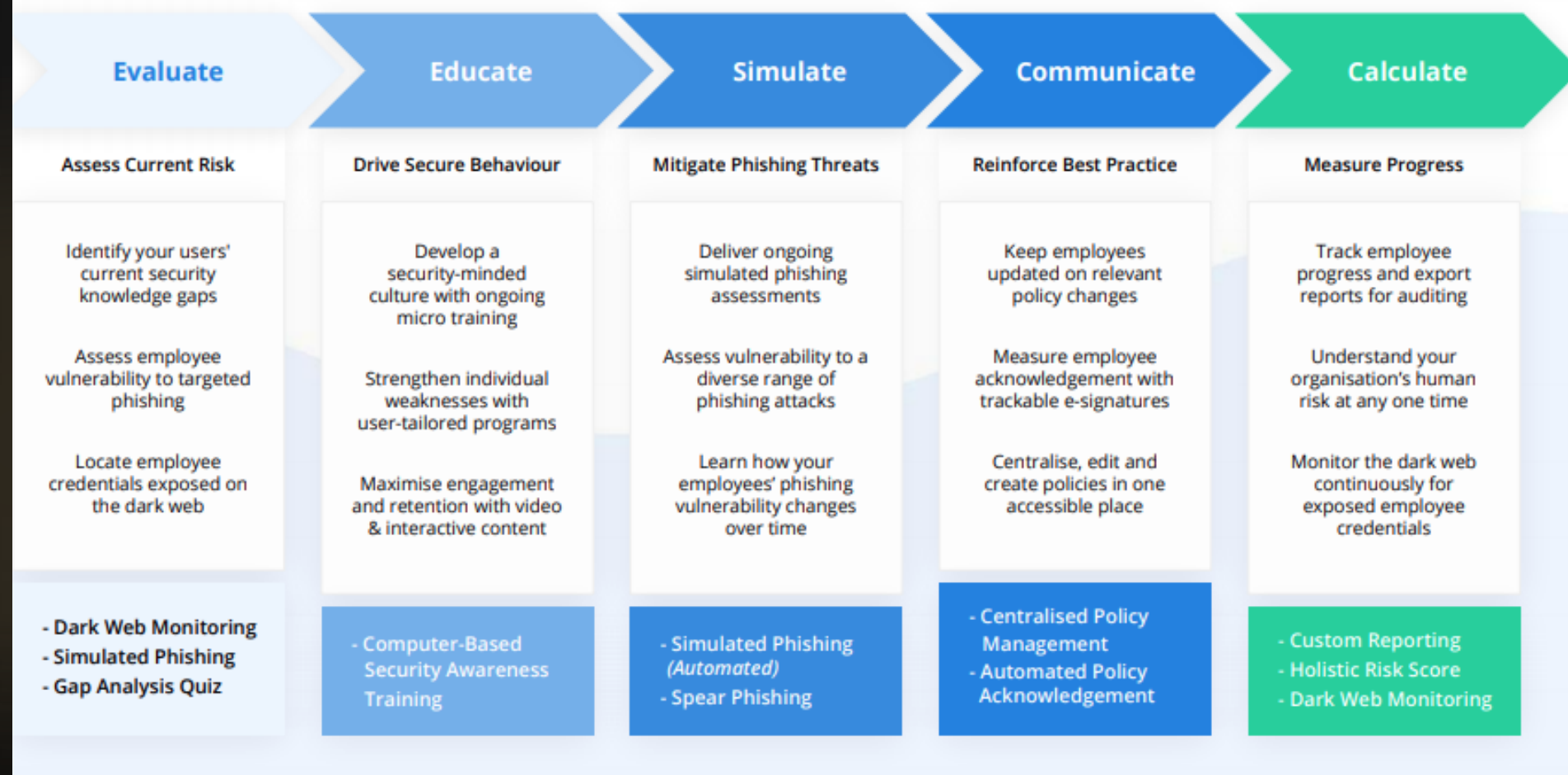
Data taken from Varonis, Verizon and Ponemon



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

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.





Security Awareness Modules



uLearn



uPhish



uBreach



uPolicy



uLearn



uLearn is a **user-focused security awareness training solution** that helps organisations drive secure employee behaviour.

Packed with an extensive library of interactive, video and blog-style content, uLearn offers engaging and continuous computer-based training - easily managed through intelligent automation.

With uLearn, you can:

- Quickly deploy a continuous security awareness training programme
- Reduce the likelihood of human-caused data breaches
- Develop a security-minded culture that can combat modern-day threats
- Cut remediation time and cost caused by internal cyber incidents
- Aid your efforts in achieving regulatory compliance

Some Key Features:

- **Intelligent automation** that eliminates repetitive admin tasks and ensures continuous user training
- **Extensive library** of infosec, compliance and custom-built courses - with new additions each month
- **Individually-tailored programmes** that identify and strengthen the user's largest knowledge gaps first
- **Bite-sized courses** - including video, interactive and blog-style content
- Easily view user progress from your **data-driven dashboard**

How uLearn works

Evaluate - Educate - Simulate – Report



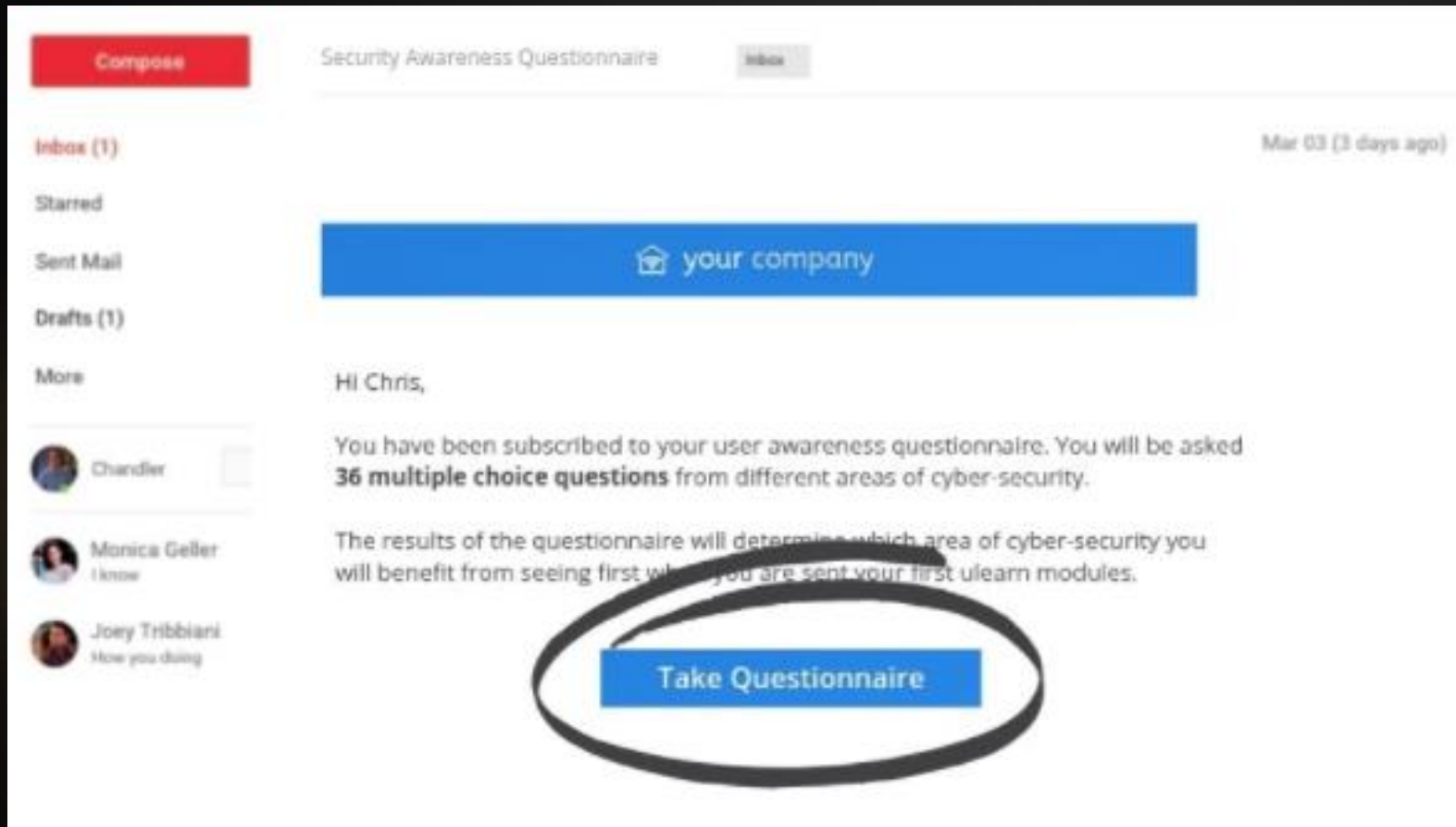
With uLearn, your users will receive a bespoke security awareness training programme that is unique to their individual infosec vulnerabilities - with the option of deploying phishing simulations to provide practical risk assessments.

To achieve this, uLearn breaks your users' training down into a simplified four-pronged approach:



1. Evaluate - Determine your users' risk profile

To start off, uLearn conducts an initial risk assessment on your users to determine their individual knowledge gaps. We call this the gap analysis questionnaire.

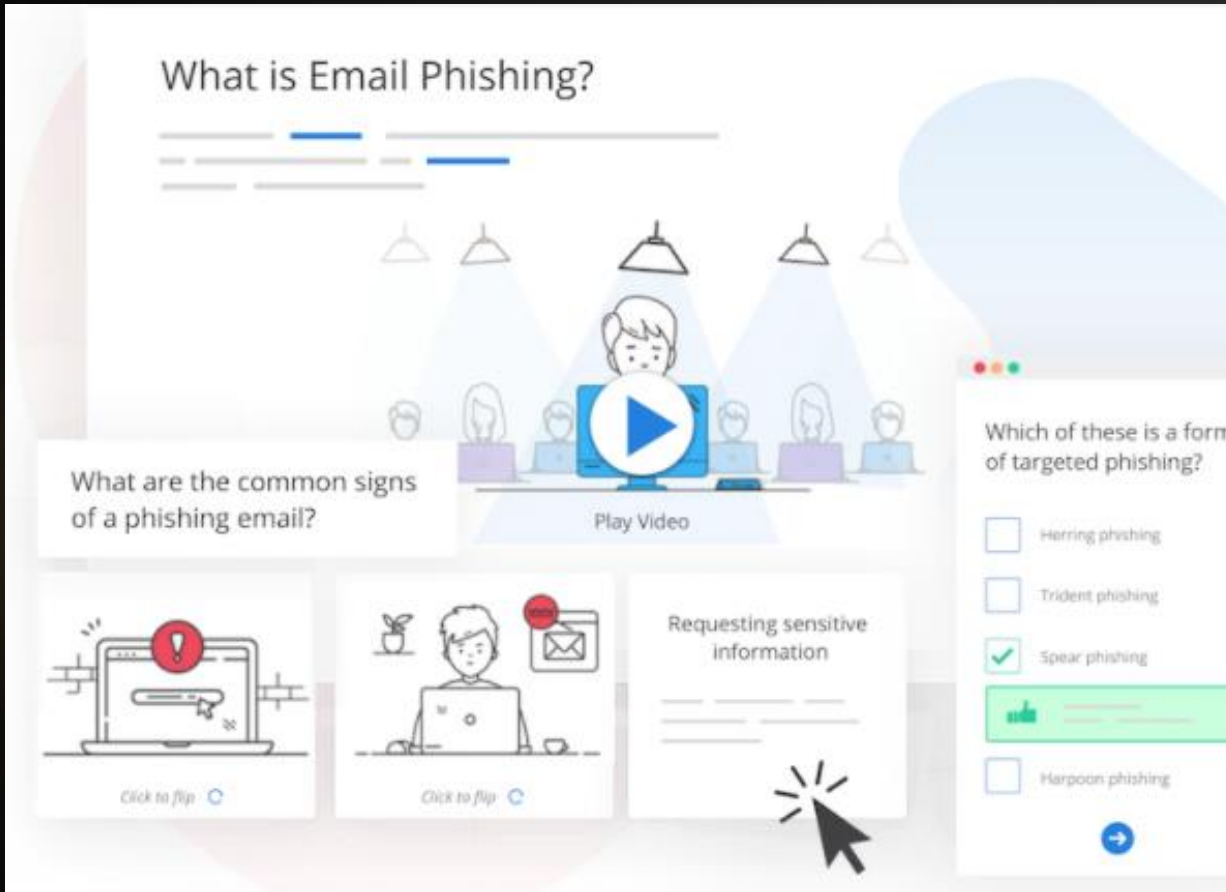


How the gap analysis works:

- **Invitation:** Your users will receive an email invitation to their questionnaire, which they can start at a time convenient for them.
- **Assessment:** Once started, your users will be quizzed on 12-core areas of infosec best practice, with this multiple-choice assessment lasting approx. 10 minutes.
- **Course enrolment:** Using the results from the gap analysis stage, uLearn will automatically craft a 12-month training programme unique to each user - with weaker subjects (e.g., phishing, passwords etc.), being deployed first.

2. Educate – Empower your users

Now your users' programmes have been created, uLearn will automatically enrol each user onto their first course.



Quick overview of your users' 12-month training programme:

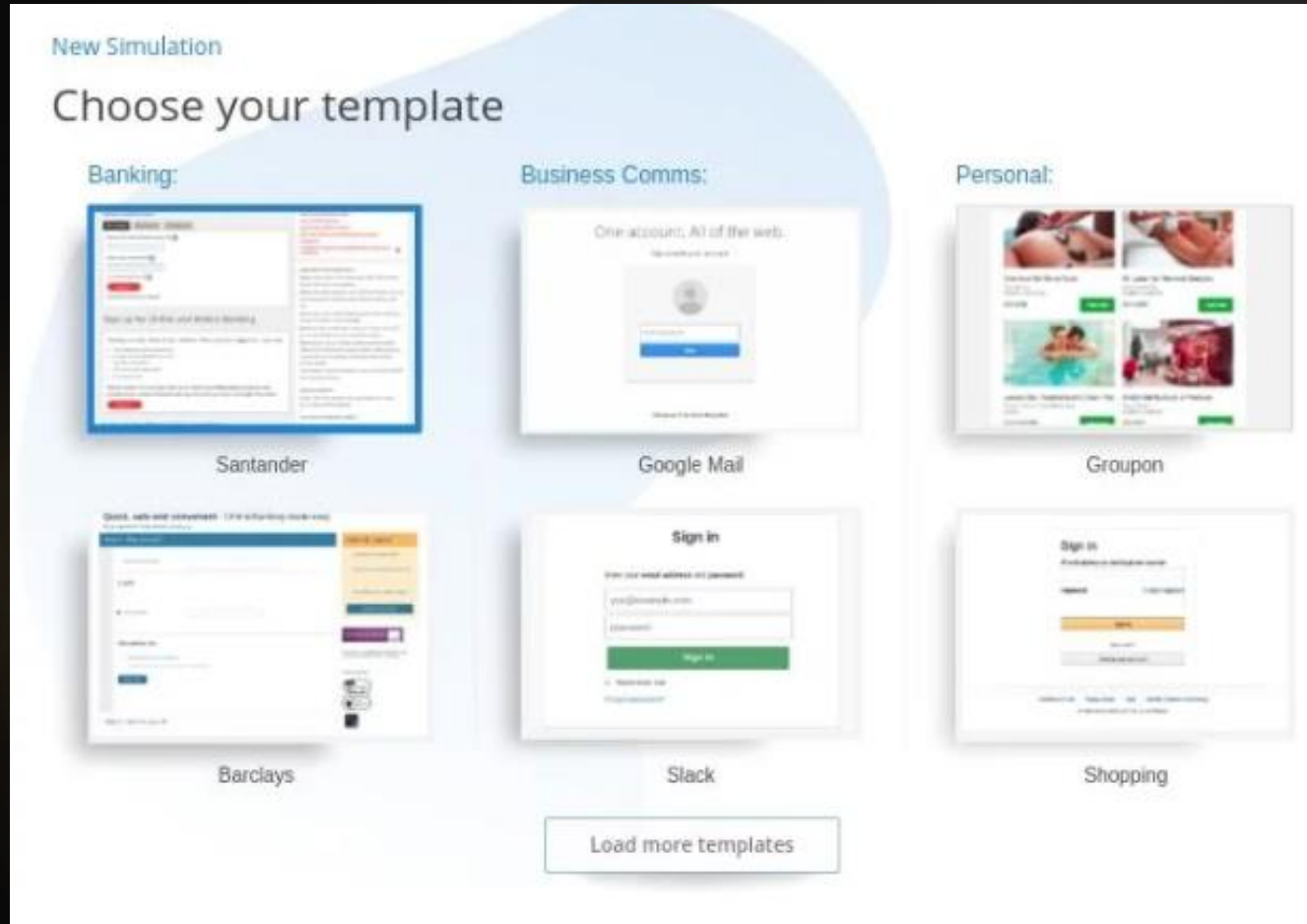
- **Prioritised courses:** Your users will receive courses that match their weakest areas first (e.g., user scored weakest in 'phishing' during the gap analysis stage, therefore, their first course will be 'Phishing Awareness for Beginners')
- **Automated invitations and reminders:** To keep your training continuous, efficient and admin-lite, uLearn will send automatic course invitations to your users, as well as reminders for outstanding courses.
- **Regular bite-sized courses:** Your users will be educated on various infosec and compliance best practice, with AutoEnrol deploying one bite-sized course per month (this frequency can be customised by the admin).
- **Engaging & jargon-free content:** uLearn courses come with video, interactive and blog-style content to engage different styles of learning, whilst avoiding confusing tech jargon.

3. Simulate – Test your users' learning progress

To ensure your users have improved their security behaviour, you're able to launch targeted simulated phishing tests using the simulation tool, uPhish.



Assess user vulnerability with uPhish:



- **Realistic phishing templates:** Your ever-growing library of phishing templates come with pre-made emails and landing pages, replicating trusted organisations and services.
- **Custom-built templates:** Create your own custom phishing templates, useful for targeted campaigns that impersonate internal communications.
- **Automated simulations (AutoPhish):** Send regular phishing campaigns to ensure user progress over time, with fully automated campaigns.
- **Real-time tracking:** Track real-time opened, clicked and compromised rates of your users to determine how they would react to a real-life attack.
- **Granular reporting:** Develop a clear risk profile of your organisation and individual users by digging deep into uPhish's in-depth reporting metrics.

4. Report – Aid your efforts in regulatory compliance

As your users progress through their training courses, you'll be able to view key insights of your organisation's uLearn performance straight from your data-driven dashboard.





uPhish is an **intuitive cloud-based phishing software** that enables you to quickly assess user vulnerability towards real-world phishing attacks.



With uPhish, you're able to identify which users are susceptible to both common forms of phishing and highly-targeted forms of 'spear phishing'.

With uPhish, you can:

- Accurately determine user vulnerability towards phishing
- Identify users that need urgent phishing awareness training
- Reduce the likelihood of users falling victim to future phishing attacks
- Develop a security-minded culture in your organisation

Key Features of uPhish:

- **Automated phishing (AutoPhish):** uPhish can deploy regular phishing simulations with our new 'AutoPhish' feature - allowing you to assess user performance over time.
- **Realistic template library:** Discover a library of phishing emails and landing pages impersonating trusted organisations, banks and more.
- **Create custom emails and landing pages:** Craft your own simulated phishing campaigns, impersonate internal communications and more.
- **Inline training:** Automatically send out additional training content to users who become compromised in phishing simulations.
- **Real-time tracking:** See how your users interact with your simulations in real-time, giving you a key insight in how users will perform during a real attack.
- **In-depth reporting:** View the individual performance of your users or assess your organisation in departments or as a whole - with custom reporting.

Key Features - AutoPhish

When the AutoPhish setting is enabled, uPhish will automatically deploy phishing simulations based on a frequency set by your IT admin (every X weeks).



uPhish - Auto Phish

Enabled:



How many weeks between simulations:

4

Only send between working hours?:



Exclude groups from receiving simulations?:

Head Office x

Exclude certain templates in simulations?:

Submit

You're also able to choose which templates you would like to exclude (both custom or pre-made), what groups of users you would like to exclude, and whether users should only receive simulations during work hours.

Key Features - Realistic template library

uPhish comes packed with an extensive library of pre-made templates, allowing you to quickly deploy realistic campaigns with ease.

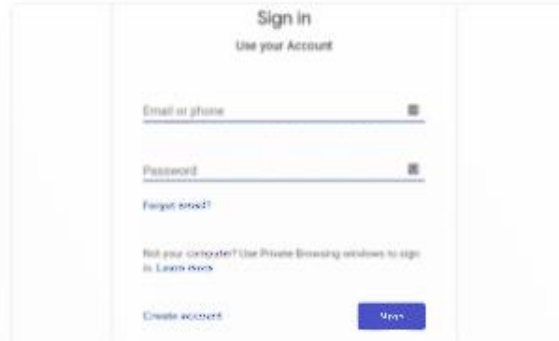


uPhish - Create Simulation

Choose your theme



Desktop



Browser



Shopping - 1



Remote



Banking - 1



Banking - 2

These templates impersonate the likes of Microsoft, Amazon, Google and many more.

Once selected, you'll be able to tweak certain settings in your chosen template (e.g. subject line, sender address) if you wish.

Key Features - Create custom emails and landing pages

Alongside your pre-made uPhish templates, you can create your own emails and landing pages and add them to your personal template library.

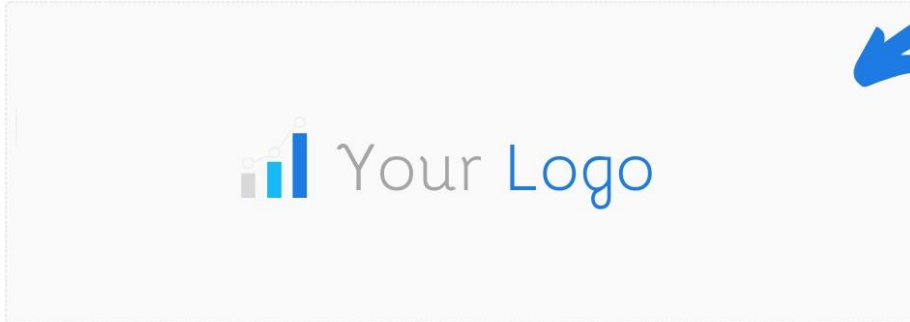


uPhish - Custom Landing Page - Create

Template Name:

Background Colour ▾

Header Image:



*Customise your emails
and landing pages*

Header Text:

Sign in to your account

Username Placeholder:

These can be used to test your users with targeted phishing attacks that impersonate employees within your company (an increasingly prevalent form of phishing)

Key Features - **Inline training**

You can choose to automatically enrol users who become compromised in phishing simulations onto additional training. You can choose from any of the courses from the library, use the purpose-built Phishing Micro Training module, or even create your own!

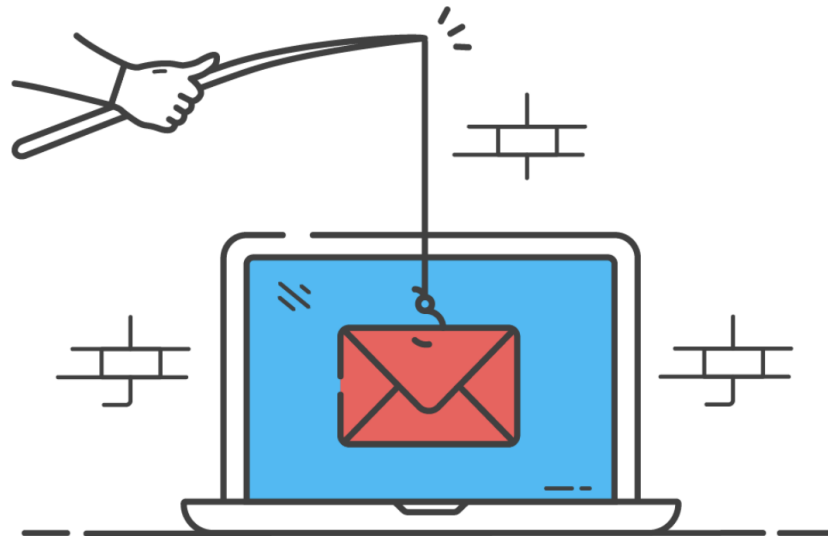


Why am I on this course?

You have been sent this course because you were compromised in a phishing simulation.

This phishing simulation was sent to you by your IT department, and is intended to test the readiness of your company or team to respond to real-life phishing scams.

The next slides will tell you more about the danger posed by phishing attempts, and how you can avoid falling for one in the future.

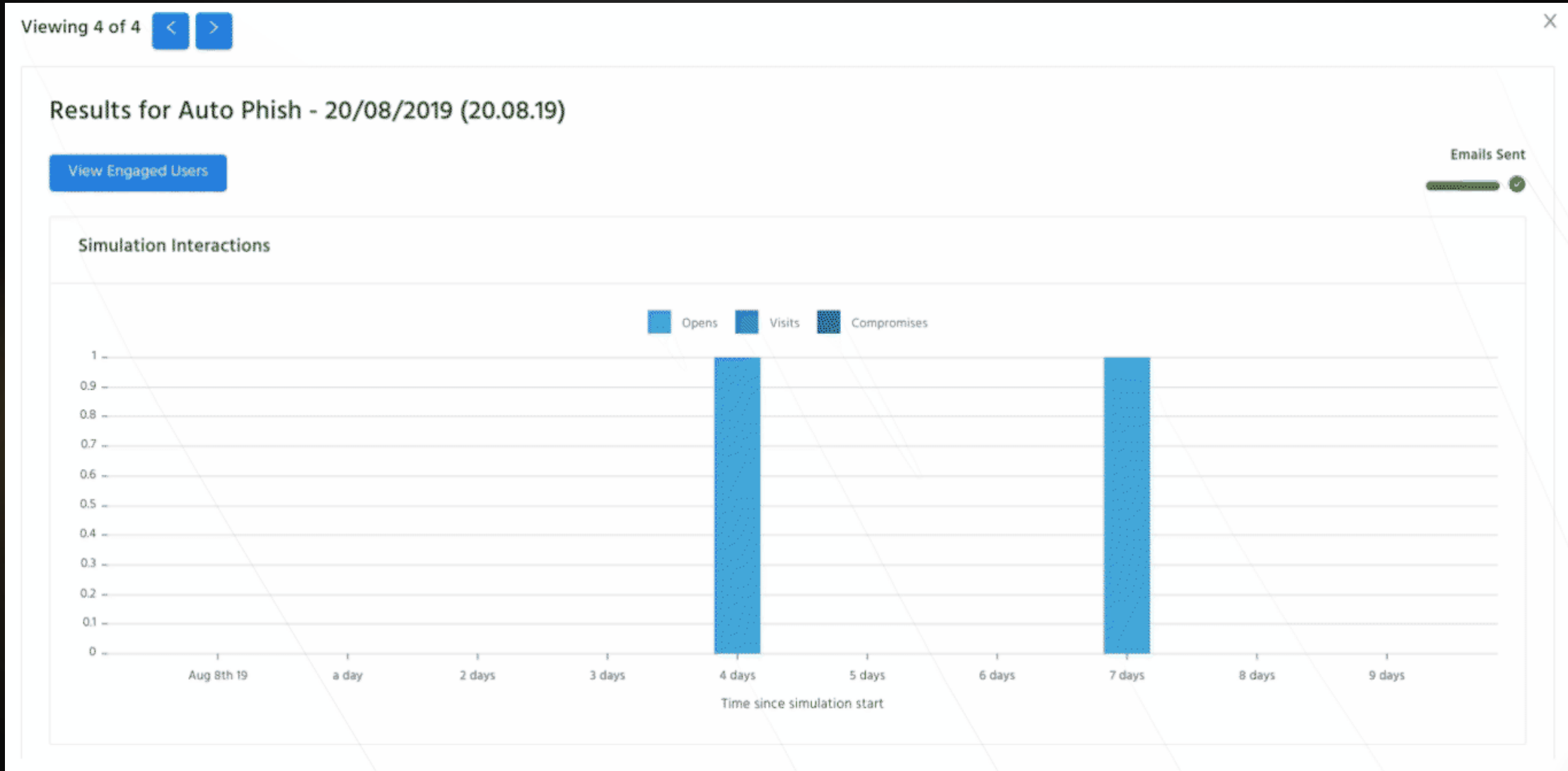


Next



Key Features - Real-time tracking

Once you have launched a uPhish simulation, you'll be able to view the real-time performance of your users, including how long it takes for them to perform each action (i.e., open, click, compromise).

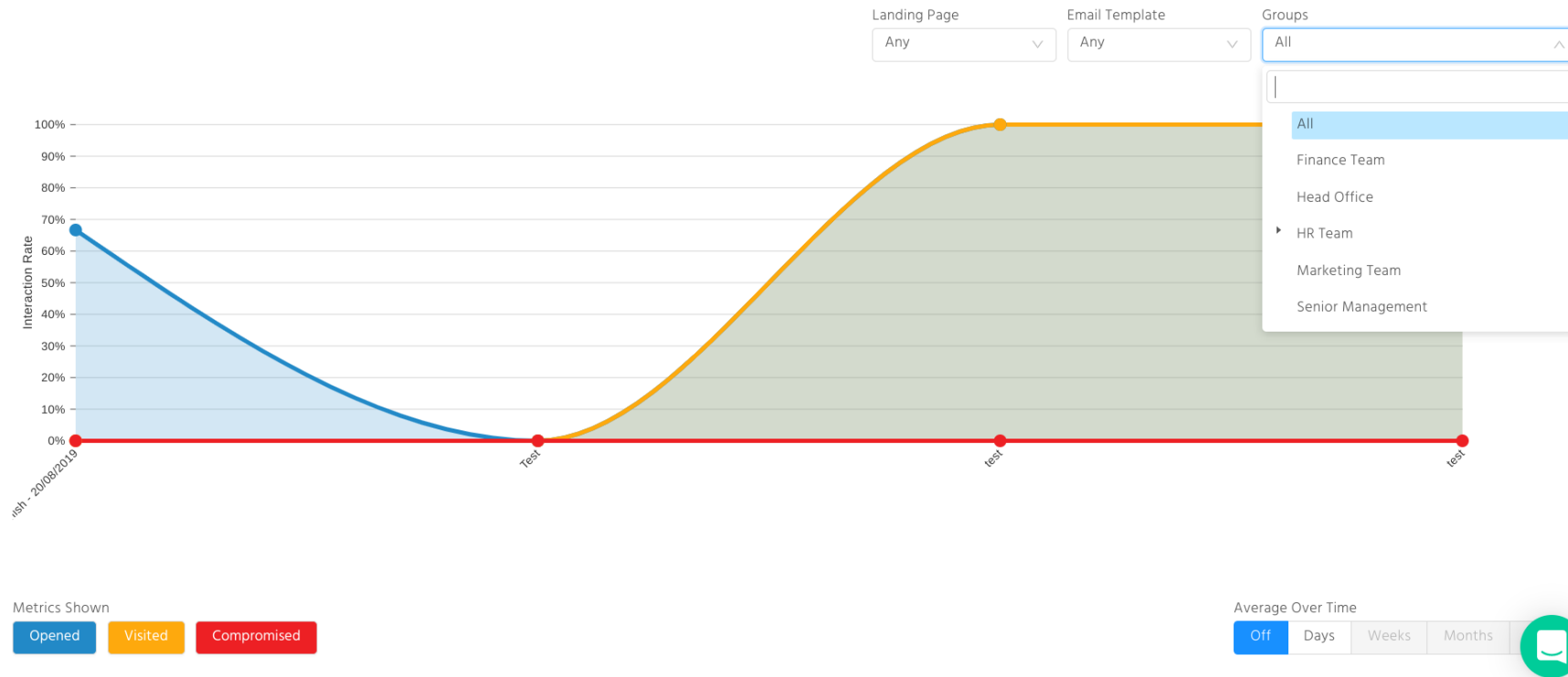


Key Features - In-depth reporting

From your 'Simulation Performance' in the 'Reports' sections, you can view and filter different metrics for your simulations.



Simulation Performance



You can filter by groups, templates, and the average opened, clicked and compromised rate over time.



uBreach enables you to **quickly identify exposed employee email accounts and identities** that have been publicly disclosed online via third-party data breaches.



With billions of credentials present in data dumps, paste sites and hacking forums, employees that sign up to third-party services with their work email address could be leaving your organisation at huge risk of social engineering, business email compromise (BEC) and other damaging attacks.

With uBreach, you can:

- **Identify exposed employee accounts:** uBreach identifies accounts that are exposed on paste sites, data dumps and hacking forums
- **Locate what employee data is exposed:** Common data includes email addresses, passwords, usernames etc.
- **Help prevent data loss:** Locating these at-risk accounts enables you to safeguard users from social engineering and BEC attacks
- **Obtain actionable steps:** with our security awareness software, uLearn, enables follow-up user training on security best practice

Key Features of uBreach :

- Quick web search enables you to rapidly identify exposed accounts
- Gathers high-level data (i.e., number of exposed accounts & source of breach) neatly into your dashboard
- View each user's exposed data breakdown from their profile
- 100% free with your subscription

How uBreach works:

Step One: Conducts a deep web search through data dumps, paste sites and hacking forums

Step Two: Identifies users that have had account information exposed online

Step Three: Collates your users' results into an easy-to-digest format, accessible from your dashboard



uPolicy allows you to **easily create and manage your company's policies.**

Having the right policies is essential for protecting your company. Policies help you set out your expectations for your employees in terms of security and their conduct in the workplace, as well as meeting compliance requirements and reducing risks.



With uPolicy, you can:

- Establish rules, standards and best practices for your employees and workplace
- Ensure policies have been read and signed by all end-users
- Contribute to a security culture and build a safe environment at your workplace
- Aid your efforts in achieving regulatory compliance

Key Features of uPolicy :

- **Pick ready-to-go policies for your company:** With our library of security policies that meet industry standards you won't have to waste time writing policies from scratch.
- **Customise policies or create your own:** You can customise our policy templates as you wish, or upload entirely new ones to meet your needs.
- **Upload your existing policies:** Upload PDF files to transfer your existing policy set to the uPolicy library.
- **Easily send out policies to your end-users:** Choose whether to send out policies to all users, individual users, or just to certain groups or departments, and ensure smooth roll out in just a couple of clicks.
- **Manage signing of policies:** Once you have sent out your policies for signing, you can see how many users have signed the policy straight from the uPolicy dashboard.

The Policy Editor

You can write and edit policies using the Policy Editor. The editor allows you to format text, insert hyperlinks and rename your policy as you wish.













Create A Policy

* Policy Name :

Acceptable Use Policy

Create your policy :

B *I* U  H1 H2    Normal       

Acceptable Use Policy

1. Overview

Most businesses now depend on computers and mobile devices as part of their daily business operations. It is essential, however, to ensure that computers and devices owned or controlled by the business are used in an appropriate, safe and secure manner.

Inappropriate or insecure use of company computers and devices could lead to a malware infection, a breach of data, or damage to the company reputation. This is why an Acceptable Use Policy is essential, as it set out clear rules on the acceptable use of company computers and devices.

2. Purpose

The purpose of this policy is to set out rules on the acceptable and secure use of computers and mobile devices owned, leased, or otherwise controlled by the company.

3. Scope

This policy applies to all employees, contractors, temporary workers and any other personnel that may use computing devices or network resources owned, leased or controlled by the Company or on behalf of the Company.

4. Policy

Viewing and sending out your policies

Policies that you have created - whether custom or from the template library - will appear on the View Policies page.



uPolicy

Select all policies

Search for policies

Search for a policy

Actions

+ Create Policy

Policies

<input type="checkbox"/>		Recipients	Visited	Signed	Compulsory	
<input type="checkbox"/>	Acceptable Encryption Policy	1	1	0	False	>
<input type="checkbox"/>	Anti-Malware Policy	0	0	0	False	>
<input type="checkbox"/>	Anti-Social-Engineering Policy	0	0	0	False	>
<input type="checkbox"/>	Automatically Forwarded Email Policy	0	0	0	False	>
<input type="checkbox"/>	Clean Desk Policy	0	0	0	False	>
<input type="checkbox"/>	Clean Desk Policy	0	0	0	False	>
<input type="checkbox"/>	Breach Response Policy	0	0	0	False	>
<input type="checkbox"/>	Dial-In Access Policy	0	0	0	False	>

Policy actions (all selected)

Policy actions

Select policy

Use the action button to the right of any policy to edit, view, delete or send out the policy. You can also select multiple policies using the check boxes on the left, and then use the top Action button to send out multiple policies at once.

How to see who has signed a policy

You can view who has signed a policy by clicking on the policy on the View Policies page. This will open the policy details window. Click the Recipients tab to see who has signed the policy.



Acceptable Encryption Policy

Search for a user



<input type="checkbox"/>	Recipient ▾	Status ▾	
<input type="checkbox"/>	Alex Thomson alex.thomson@[REDACTED]	Visited	>
<input type="checkbox"/>	Neil Woods neil.woods@[REDACTED]	Signed	>
<input type="checkbox"/>	Kerry Rowland kerry.rowland@[REDACTED]	Signed	>
<input type="checkbox"/>	Bob McCartney bob.mccartney@[REDACTED]	Signed	>
<input type="checkbox"/>	Morgan Freeman morgan.freeman@[REDACTED]	Signed	>

<

1

>



Self Managed	Managed	Add-Ons
<p>Manage your cyber security strategy internally with full access to all the modules through our user friendly dashboard.</p>	<p>Don't have the time to create your custom courses or manage the back end?</p> <p>Not a problem, we can do it for you!</p> <p>We will fully manage all modules for you, send a phishing simulation, 1 custom course, monitor your data breaches, and send your monthly reports.</p> <p>You also have full access to the dashboard.</p>	<p><u>Courses</u></p> <ul style="list-style-type: none"> - Bespoke Multiple Choice** - Bespoke Video presentation** <p><u>Other</u></p> <ul style="list-style-type: none"> - Policy Creator & Distribution** - Multiple Phishing Simulations per month
£1.75 per license (monthly)*	£100 + 1.50 per license(monthly)*	Contact Us

* All prices exclude VAT. Minimum of 10 licenses. Annual commitment
 ** Content must be provided by client

Where would I use it?

Just a few examples on how you would use the e-Learning platform in your business.



**INDUCTION PACKAGE FOR
NEW STARTERS**

TEST INTERNAL SECURITY

**HAVE A RECORD OF
TRAINING FOR YOUR STAFF**

**NOT LIMITED TO CYBER
SECURITY, CREATE YOUR
OWN COURSES**

**INTRODUCTION TO NEW
SYSTEMS AND PROCEDURES**

**CHECK IF STAFF
CREDENTIALS HAVE BEEN
COMPROMISED**



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

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

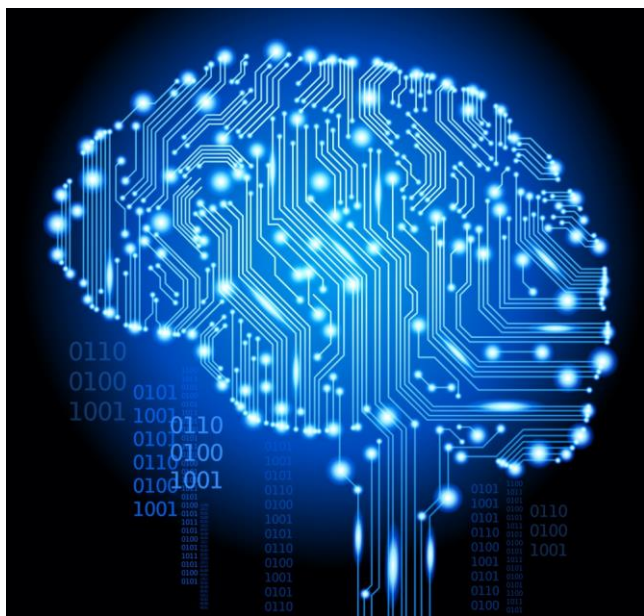
We'll identify your employees' compromised and stolen data that is exposed on the dark web and accessible to attackers.

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.



Q&A TIME



Thank You!



WWW.LEVELUPNETWORKS.COM



HELLO@LEVELUPNETWORKS.COM



0203 695 7554 (OPTION 1)

