

# Phishing Simulation & Security Awareness Platform

Fully Automated service that produces results Simple. Powerful. Affordable.

Did you know?

95% of all cyber security issues are caused by human error according to the - World Economic Forum Global Risk Report 2022.

All it takes is one employee to cause a data breach.

A focus on improving employee security strength will help business to significantly uplift their Cyber Security Posture.



\*\*\*

### **Turn Your Employees into a Superhuman Firewall**



# **Annual Cybersecurity Training**

Set the foundation each year with an overview and assessment of the most important cybersecurity practices.

### **Monthly Newsletters**

Security newsletters sent monthly to keep users up to date with the latest cybersecurity trends and consistently reinforce security awareness.

### Weekly micro-training video, quiz

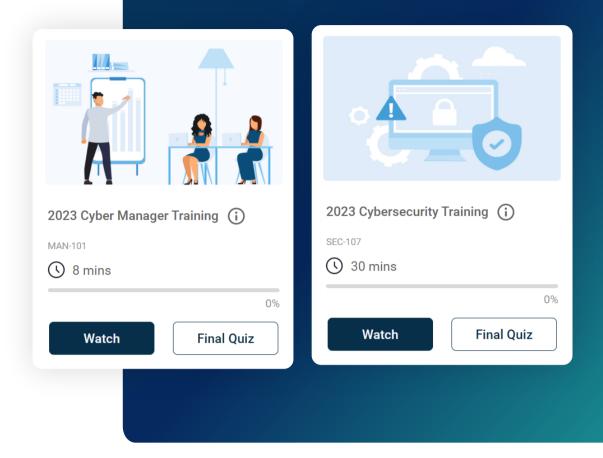
Weekly 2-minute micro-training video & short quiz to keep users continuously trained while enhancing their Employee Security Score (ESS).

# **Phishing Simulation**

Routine simulated phishing has been proven to minimize the risk of end-users falling victim to a malicious phishing attempt.

Routine phishing instills into our users the very behaviors of IT professionals before they click on any link so that even on the most chaotic of days, they're ready.

### Dark Web Monitoring





Proactively monitor the dark web for compromised account data. The sooner end-users are notified of a breach, the sooner they can change their passwords.



### **Written Security Policies**

#### Policy acknowledgment

Security policies are key to establishing expectations and explaining repercussions to protect your client organizations. Our document management portal contains a variety of customizable security policies from BYOD to Security Incident Response.

Security policies protect your organization's critical information/intellectual property by clearly outlining employee responsibilities with regard to what information needs to be safeguarded and why.

### **Security Documentation Portal**

Enforce Employees to electronically sign or acknowledge that they have read and agree with the policies. Capture and record any security incidents.

Track and maintain all third-party service providers.

	Policy 个	Name	Description	Download	Acknowledge
Jacob Doe	1	Written Information Security Policy	Written Information Security Policy (WISP) that defines the administrative, physical and technical safeguards to protect personally identifiable information (PII) and sensitive company information.	Ŧ	5
	2	Termination Policy	Policy defines the steps required to revoke both physical and system access to the organization's facilities and network resources when terminating an employee.	Ŧ	8
My Dashboard 🖒	3	Security Incident Response	Procedures for reporting, responding to and managing security incidents.	Ŧ	5
🗊 Newsfeed	4	Sanction Policy	Policy governs employee sanctions and disciplinary actions for non-compliance with the WISP.	*	8
	5	Network Security	Policy describes the physical safeguards applicable for each server, desktop computer system and wireless computer system used to access, transmit, receive and store PII and sensitive company data to ensure that appropriate security is maintained and that access is restricted to authorized employees.	÷	5
	6	Access Controls	Policy to assure that systems containing PII and/or sensitive company data are accessed only by those persons or software programs that have been granted appropriate access rights.	Ŧ	8
	7	Computer Use	Policy to ensure that employees understand what functions should and should not be performed on The Company's computers and network to maximize the security of PII and sensitive company data.	Ŧ	8
	8	Disposal Procedure	All media containing PII and sensitive company data, will be disposed of in a manner that destroys the data and does not allow unauthorized access to the data.	4	5
	9	BYOD Policy	Policy describes the appropriate safeguards to protect PIII and sensitive company data on employee personally owned devices.	Ŧ	5
	10	Facility Security Plan	Policy defines the procedures that will limit physical access to PII and sensitive company data and the facility or facilities in which such systems are housed.	4	

# **Security Risk Assessment**

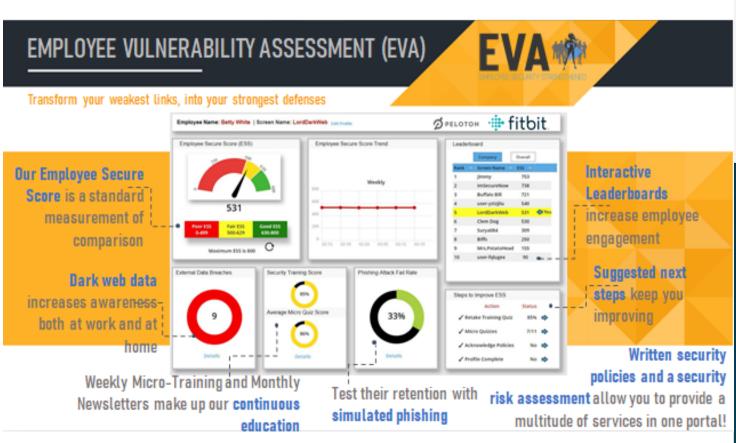
Security Risk Assessment (SRA) assesses cyber security based on NIST standards, identifies

the gaps associated risks, and provides recommendations for improvement

### **Employee Vulnerability Assessment (EVA)**

EVA identifies the human vulnerabilities and related risks. As a visual dashboard, provide security metrics such as:

- Employee Secure Score
- List of employees posing the greatest risk
- Phishing Attack Fail Rate
- Security Training Score
- Micro Quiz Score
- Security policy review and
- Dark web scan results in terms of external Data Breaches



# **Proven Return on Investment**

From the very first phishing simulation, actively improves your organization's Security Awareness.

### Don't just take our word for it; we back it up with data.

### 50% Up to half of your employees will get phished during initial test.

# **2X**

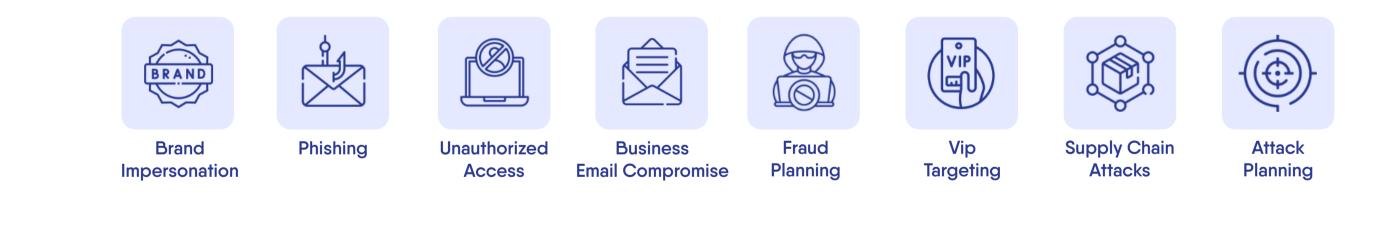
Reporting rates double within the first six months, both for phishing simulations and real phishing threats.

### 5%

Click rate drops dramatically on average in 12 months' time. After just 6 months, this will already have dropped to 20% on average.



### **Reduce the risk of cyber threats with Phishing Simulation & Security Awareness Platform**



#### **Testimonials**

Cyber awareness has increased significantly as the number of successful phishing click rates has decreased

**CISO Financial Services** 

Very powerful reporting to get insights on our Human security and present it to senior execs **Security Manager Health** 

### Contact us and request for a free demo

www.cyber-forte.com 

info@cyber-forte.com

