

# Cyber awareness training solution - CyberProtect

## Background

Since the start of the COVID-19 pandemic, the World Health Organisation has reported a fivefold increase in cyber-attacks. This is the same trend that is being experienced in companies across the globe.

Below are some key statistics around what happens in the world within 1 internet minute:



**1,5**  
cyberattacks on computers with an internet connection per minute



**16 172**  
records are compromised every minute



**375**  
new records are compromised every minute



**1**  
COVID-19 fraudulent domain is blacklisted every 15 minutes



**35**  
COVID-19 spam emails are analysed per minute

## Why CyberProtect Security Awareness Training?

**Identify Risk** - The solution identifies risk through threat simulations, and knowledge assessments.

**Change behaviour** - Deliver targeted education driven by threat intelligence to the right users.

**Reduce exposure** - Turn your employees into a strong last line of defense and make them part of your team.

**Business intelligence and integrations** - Get the granular and high-level visibility you need into your users' assessments, simulated attacks, and training assignments.

## CyberProtect provides these benefits:

- Threat intelligence that helps organisation stay ahead of attackers
- Continuous improvement of the cyber resilience level of your organisation
- Provide periodic contact moments to discuss cyber-related topics with our cyber security experts

# System offering and features

## Monitoring and reporting

- Comprehensive, but easy to use **security dashboard with reports and analytics** to show the performance of security awareness training campaigns and measuring how well employees are improving over time.

## Testing

- There is a range of security testing on offer, with videos, posters, images and articles to get people engaged with security concerns.
- **Range of tests** to measure employee's security awareness outside of simulated phishing with '**CyberStrength**' assessment platform.

## Campaigns and training material

- Well-researched and **interactive training modules** with a wide selection of videos, posters, images and articles to help engage users to remember security awareness materials
- Customers highly praise the training material on offer, particularly the **engaging video content**.
- Capable solution for companies looking for **ongoing security awareness training with engaging materials**
- **Training modules** are made for **different sectors** to help meet specific training needs, with ongoing and updated content

## Phish alarm

- **Phish Alarm** feature is an email client plug-in which allows employees to report suspected phishing attacks

## Simulations

- Range of **simulated cyber attacks** to test how security aware employees are, with phishing, USB and SMS simulations with customisable templates

# Contact us

Should you have any queries, please do not hesitate to contact our team.



**Kudakwashe Charandura**

**M:** +27 (0) 82 868 3689

**T:** +27 (0) 11 230 0600



**Bekinkosi Rikhotso**

**M:** +27 (0) 82 868 3689

**T:** +27 (0) 11 230 0600

For general enquiries please contact us at

**E:** [cyber@sng.gt.com](mailto:cyber@sng.gt.com)



© 2020 SNG Grant Thornton - All rights reserved.

"Grant Thornton" refers to the brand under which the Grant Thornton member firms provide assurance, tax and advisory services to their clients and/or refers to one or more member firms, as the context requires. SNG Grant Thornton is a member firm of Grant Thornton International Ltd (GTIL). GTIL and the member firms are not a worldwide partnership. GTIL and each member firm is a separate legal entity. Services are delivered by the member firms. GTIL does not provide services to clients. GTIL and its member firms are not agents of, and do not obligate, one another and are not liable for one another's acts or omissions.