Cyber security

Operate with confidence
CGI phishing defence services

Contents

We work with leading organisations across the commercial and government sectors in the UK, Canada, USA, Australia and Europe.

Cyber security is part of everything we do

We have over 1,700 cyber security experts globally and one of the largest cyber security practices in the UK helping clients manage complex security challenges with a business-focused approach, protecting what is most valuable to them.

Ensuring organisations are resilient against cyber-attacks and protecting data accordingly has become one of the most important challenges facing senior management.

We work with leading organisations across the commercial and government sectors in the UK, Canada, USA, Australia and Europe.

We understand security from every angle - technology, business and compliance. Our specialists build cyber security into organisations to drive agility, efficiency and competitive advantage. Our services help organisations with privacy, business resilience and by enabling innovation.

Assess the risk:

Helping clients to assess and manage security vulnerabilities so they can be confident their organisation is secure, compliant and ready to grow.

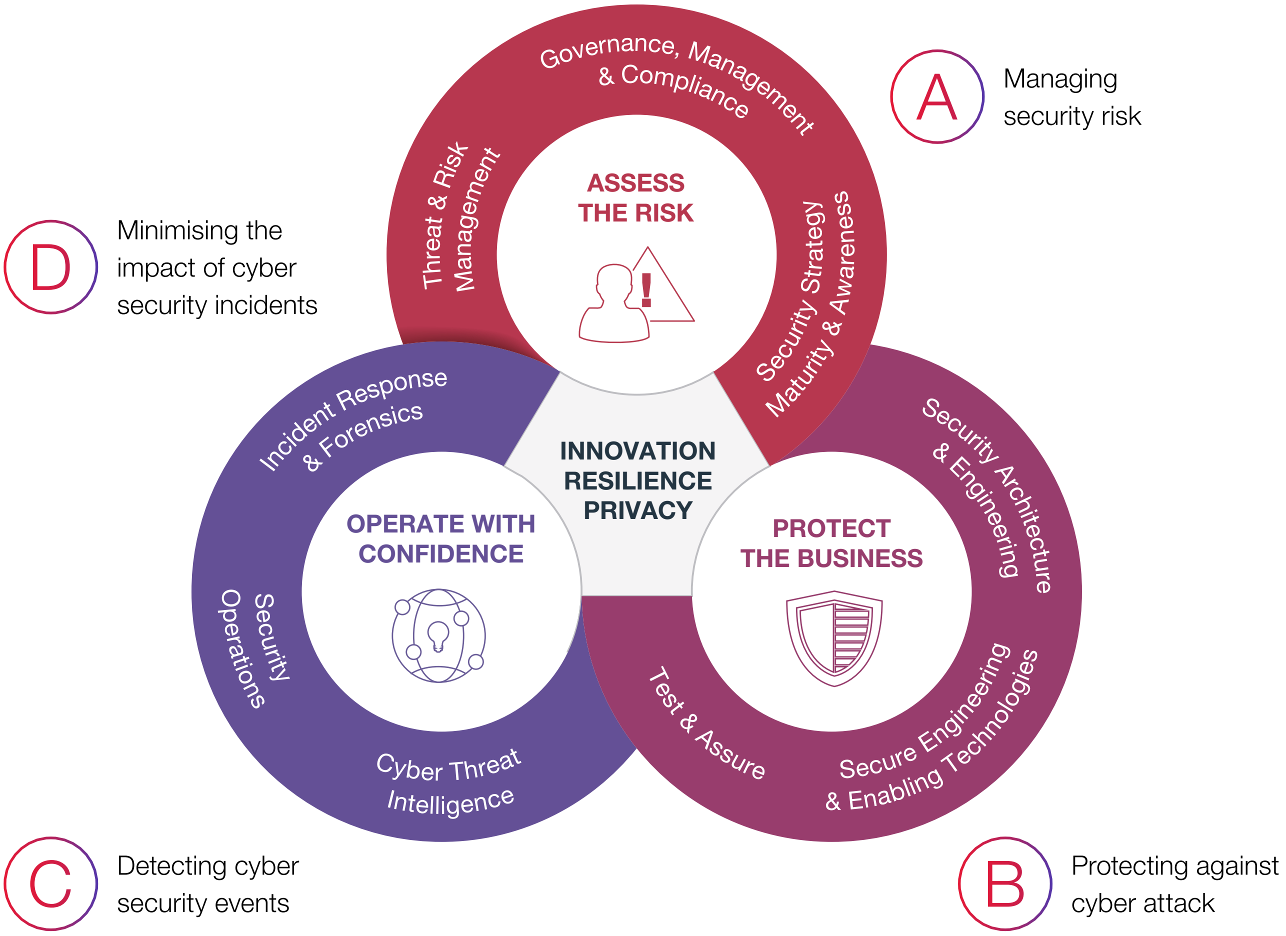
Protect the business:

Helping clients to build in security early, and test its ongoing effectiveness - securing the systems an organisation relies on to operate and grow.

Operate with confidence:

Helping clients to monitor prevent and respond to security attacks in a reliable and cost effective way.

Cyber security wheel



Governance, Management & Compliance
Threat & Risk Management
Security Strategy Maturity & Awareness
ASSESS THE RISK
A
Managing security risk
D
Minimising the impact of cyber security incidents
Incident Response & Forensics
Security Operations
Cyber Threat Intelligence
OPERATE WITH CONFIDENCE
INNOVATION
RESILIENCE
PRIVACY
Security Architecture & Engineering
Test & Assure
Secure Engineering & Enabling Technologies
PROTECT THE BUSINESS
C
Detecting cyber security events
B
Protecting against cyber attack

Educate

Phishing education services (simulation-PhishMe)

One of the biggest threats against any organisation is phishing emails. No matter how good your perimeter defences are, phishing emails can still reach employees and provide attackers with access to your network.

Phishing is one of the main attack vectors that allows an adversary access into your networks. There have been numerous high profile and costly attacks started this way. When your email gateway fails to identify a phishing email your last line of defence is your employees – but are they prepared?

How it works

Our aim is to improve an employee's ability to identify suspicious emails, reducing the impact a phishing email could have on the individual and on the organisation and increase visibility via reporting aimed to be actioned at the management level. This improves the organisations resilience to the current and future cyber threats.

Customised to you

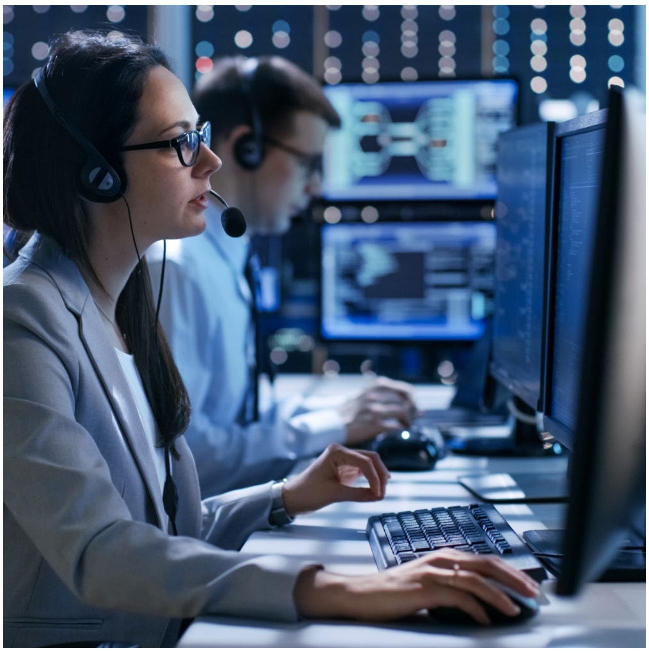
We begin by assessing your needs and creating a campaign schedule that matches your organisation's culture. This will include looking at which employees you wish to educate, the frequency of scenarios and the topics you would like to cover. We are able to identify and prioritise high-risk employees, such as the members of your finance or human resource teams. Prior to each campaign we create a real-world scenario simulating the most relevant threats. In addition, educational content relevant to that scenario is also developed to increase awareness.

If a simulated Phishing email is interacted with by an employee, then education is instantly delivered so that employees who are most susceptible to attacks are identified and provided with best-practice education. It is recommended that scenarios are run at least monthly as it has been shown to double the rate of reporting and double your resiliency score.

Educate

Reporter button

Simplify the process of reporting suspicious emails by using our reporter button. By making the process easy, it empowers the employee allowing them to proactively participate in your organisation's security program. The reporter button is easy to install and can be used on either PC or MACs with Outlook, Microsoft 365, Gmail, or Lotus Notes email toolbars. When clicked the reporter button automatically discerns whether the email is part of a phishing simulation or sent by an unknown source and sends the suspicious email to your security team or ours, as part of the managed triage service.

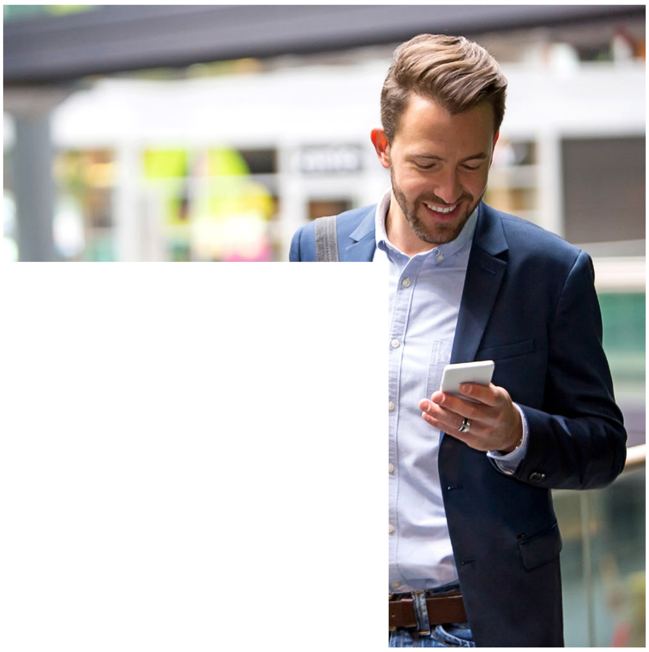


Education

Threat actors are constantly innovating and changing their tactics when attacking organisations. Our education program works alongside the phishing simulations in order to improve employee's knowledge. The education program we provide is completely customisable, progressive and allows us to tailor it to the needs of your employees.

Our education program is delivered in two ways – emails are disseminated to all employees covering a variety of security awareness topics, and further education is given to those employees who fail to spot the phishing simulation as part of the scenario. All education material is interactive, using animations, graphics, videos and informative content to keep your employees engaged.

CGI utilise a Phishing platform that can provide Intelligence Analysts with an unmatched range of cyber-attack themes, content and customisation. Information on active threats is used to continually update the Phishing Education Service, ensuring that the scenarios used are aligned to the ever-changing threat landscape. We can even provide scenarios based on phishing emails that we have seen targeting your organisation.



Benefits

We will provide you with detailed analysis and reporting for each scenario, allowing you to track the organisation's performance. This will provide you with a picture of the effectiveness and the improvements to your organisation's phishing resilience.

Following each campaign, you will receive a detailed breakdown of how your company performed. This will allow you to see how your company is increasing its:

Response rates - How many employees identified the email as suspicious:

- Time to first report
- Time spent on training

Individual responses – With the ability to highlight those personnel who require further training.

We will then use this data to inform future scenarios and target any organisational weaknesses. We can even run additional simulations targeting high risk employees.

Technical overview

To deliver a the CGI Phishing Educate (Simulation) service:

- Client provides email list for employees to target
- The reporter button is deployed to the user base
- Agree campaign theme complexity and duration with the client

CGI utilise a Phishing platform that can provide Intelligence Analysts with an unmatched range of cyber-attack themes, content and customisation.

Phishing service

LMS

All organisations need to educate their employees about cyber security risks. The Learning Management System streamlines employee computer-based training. The system allows you to manage content, report on progress, and use leading edge education programmes to develop and reinforce the behavioural change required to keep you organisation safe.

How it works

Using the Learning Management System, CGI will create an education program that fits the needs of your organisation. This will then be managed and maintained by CGI ensuring your employees are enrolled on the appropriate courses, and that they are reminded to complete their training. Reporting will then be compiled to inform you how your employees are progressing with their training.

LMS contains up-to-date training on many cyber security risks including:

- Cyber security for business
- Personal Identifiable Information (PII)
- Internet of Things (IOT)
- Malicious Links
- General Phishing
- Business Email Compromise (BEC) scams
- Data protection
- …..and many more

Modules include interactive learning activities, allowing employees to gauge their understanding. Content can also include quizzes, certificates, presentations, or points for completion in order to reinforce training.

Within this system, it is possible to upload any Cognitive Behavior Therapy (CBT) modules, lessons or learning materials that you organisation already uses in order to keep all of your online training in one place. In addition, many of the courses are available in a range of languages.

CGI will create an education program that fits the needs of your organisation.

Re-engagement

Tracking who has completed their training can be time consuming. LMS automatically tracks this information and if the employee has not engaged in the learning the system prompts them via emails to complete their assigned training modules.

This service is fully customisable with emails using your own branding and wording, helping ensure that your employees complete their activities within the specified time. Reminders can be sent out weekly, monthly, every other month or quarterly so as not to overwhelm your employees.

Reporting

Reporting is available on a number of metrics that have been listed below:

- Completion report by course
- Completion report by month
- Outgoing email report
- Individual users report
- Non-participation report

This will give you detailed information as to how your employee groups are progressing and can provide you metrics on the preparedness of your organisation.

Phishing service

Reporter button

Our Phishing Reporter button makes it easy for your employees to report suspicious emails as well as simulated email campaigns with only one click.

When employees are unsure of how to report phishing emails, they often don't report them. This leaves your Security Operations Centre without visibility of the threats entering your organisations inboxes.

Employees can often recognise suspicious emails but are not exactly sure of how to report them. Do they need to forward them onto the service desk or security team? What address do they need to forward it onto? The Phishing reporter button takes away all the uncertainty making reporting an email as easy as one click.

How it works

Improved reporting

By making reporting simple, employees feel empowered. This has been shown to lead to reporting rates at least doubling in organisations who have deployed the Reporter button. The button can quickly discern real phishing emails from those sent as part of CGI's educate campaigns, ensuring only real emails are sent to your security analysts. Increased reporting helps your security team identify the present and emerging threats, and apply timely mitigations to keep your organisation safe.

Reporter button

The Reporter email tool bar button makes it simple to report. Easy to deploy as an add-on for PCs or MACS, it works with Outlook, Microsoft 365, Gmail, or Lotus Notes toolbars. There is also a reporter for mobile available for the Microsoft Outlook app on iOS and Android.

The whole email

It is important for analysts to be able to gather as much detail as possible on the threats entering your inboxes. The reporter button helps preserve the integrity of the emails, packaging them in a standardised format, before forwarding them to the Cyber Threat Investigation team for analysis. The full email header, URL's and attachments provide analysts with all the relevant information they need to understand the threat. This allows defenders to analyse the emails and collect the information needed to block and remove similar emails.

Benefits

The Reporter button works alongside the Educate and Analyse services that CGI provide. The button can detect when the email is sent as part of an educate campaign. It notes which employees are reporting and sends personalised thank-you's, to provide positive reinforcement and keep employees engaged. It also collects reporting metrics, such as employees' responses and response times, used by both the education and analyse tools to help you understand your organisations security posture.

Employees can often recognise suspicious emails but are not exactly sure of how to report them.

Phishing service

Analyse (triage)

Our Phishing Analyse service (Triage) utilises the CGI Triage platform along with our in-house CGI specialists to help you process and analyse real phishing threats affecting organisations.

Our Security Operations Centre team quickly identifies and remediate attacks in progress and improve phishing threat analysis efficiency from hours to minutes. This frees up the manual resources previously needed to process the thousands of malicious emails reported by employees.

How it works

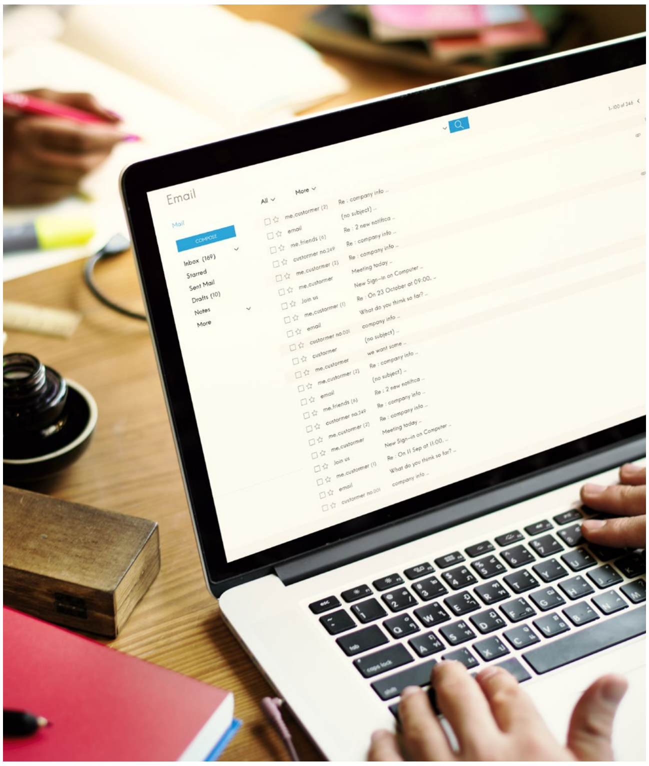
By using the CGI Triage tool we can increase your resiliency to phishing threats by automating the identification, prioritisation and remediation of phishing threats in real time. In addition, it allows us to understand the phishing specific threat and then deliver actionable intelligence, enabling a faster and more efficient response.

Clustering

CGI's Triage product has a vast and continuously updated library of rules that aid our analysts by grouping the emails received into clusters. These clusters of emails may contain the same malware payload or footprint. Once clustered they are passed through an industry-leading spam filter to classify them as false positives or known bad. Clustering and categorising benign emails helps to cut down the "noise" caused by false positives, and allowing for faster identification of malicious emails, improving response times.

The software used is cutting edge. It uses the clusters to recognise campaigns against an organisation, and can also help identify morphing campaigns – even when the subject and sender changes. Once a payload is found the software is able to auto-submit it to existing sandboxes or security tools such as Virus Total for further investigation.

This clustering also allows the analyst to collate Indicators of Compromise and rapidly send them to the upstream or downstream team for further action. Triage also allows for indicators to be shared via an API so that they may be consumed into other security tools, such as gateways, EDR or SOAR.



Our Security Operations Centre team quickly identifies and remediate attacks in progress.

New malware

New malware or phishing campaigns may not be processed by the library of reporting rules. Emails that fall into this category are highlighted to the CGI analyst team who use their expertise to manually analyse these emails and threat hunt. They will then provide feedback to the organisation of their findings to help remediate against new and emerging threats.

Feedback

In order to encourage employees to report suspicious emails feedback is provided on every reported email. Each email reported is followed up with information on whether the email contained malicious content or not.

This allows employees to feel that they have aided the organisation by reporting suspicious mail and to have played a valuable part of the phishing defence programme.

In addition, Triage collects data on who has reported, how quickly and if it was a false positive or not. Employees are given a Reporter Reputation score based on these factors and this further helps the system identify threats by noting which employees reliably inform on a real threats to the organisation.

Phishing service

Benefits

The CGI CTI team will provide you with a monthly report on your Trainge service. It will cover a number of areas helping you to understand the threat against you. It will include:

- Number of emails reported
- A break down as to how many are false positive, known malicious malware, phishing simulation and spam
- Number of reports of each type of malware
- Monthly; facilitates discussion and understanding between operations and strategic planners
- Add's flexibility to scale up and down as your business needs

Reporters

- Who in your organisation is great at reporting malicious emails
- Operational; contextual intelligence used to support Digital Forensics, Incident Response/Incident Handling and Threat Hunting
- Strategic; intelligence that supports business risk management, building maturity, capability and compliance
- Specificity
- General
- Sector
- Company

Other offerings and variations to this service to meet your individual business needs are available.

Technical overview

To deliver the CGI Phishing Analyse (Triage) service

- Client hosted or cloud environment, a scalable Azure Virtual Machine (VM);
- CGI installation and Support;
- Authenticated remote access to the Triage Server;
- Whitelisting;
- Button deployment;
- Access and Configuration of a Simple Mail Transfer Protocol (SMTP) Server

Sizing recommendations

The recommended minimum specifications are:

- **VM size:** Standard B4ms
- **Memory:** 16 GiB RAM, 32 GiB RAM recommended
- **Processor:** 4 virtual CPUs
- **Storage:** You can configure Triage to use either a local data disk or a remote PostgreSQL database to store data depending on your organization's performance and data security needs
- **Local data disk:** 1 TB (minimum) to 1.99 TB (maximum). This disk will contain Triage data, including ingested emails, configuration settings, backup dumps, and snapshots
- **Remote PostgreSQL database:** Create as a General Purpose database with a minimum of 1 TB of storage. This database will contain Triage data, including ingested emails and configuration settings
- **Network:** 1 card maximum (more than one card installed on the appliance can cause issues)
- (Optional) SSL certificate for the Triage hostname

Our specialists build cyber security into organisations to drive agility, efficiency and competitive advantage.

Our services help organisations with privacy, business resilience and by enabling innovation.

Phishing service

Vision (triage bolt on)

CGI's Phishing Service offers a further defence against malicious emails – Vision. This product enhances your phishing defences by providing a "search and destroy" capability.

When an email gets through your Secure Email Gateway it is unlikely it will be alone. Campaigns against organisations can result in hundreds of emails being sent. If the Security Operations Centre receives a report of a malicious email how does it go about locating the other inboxes that it has reached? CGI uses Vision software to search all employee inboxes, quickly removing and quarantining phishing emails.

How it works

Threat hunting

Vision makes use of potential Indicators of Phishing in an offline environment optimised for threat hunting. This allows for automated threat hunting deployed in a way that is unaffected by Microsoft's EWS throttling and separate from your mail team's production environment. This results in a fast, proactive response, reducing your organisations exposure to the threat.

Vision is not limited to searching on subjects and senders. It supports complex queries involving domains, URLs, attachment names and hashes allowing it to find even the most dangerous polymorphic attacks.

Integrated with CGI analyse capability

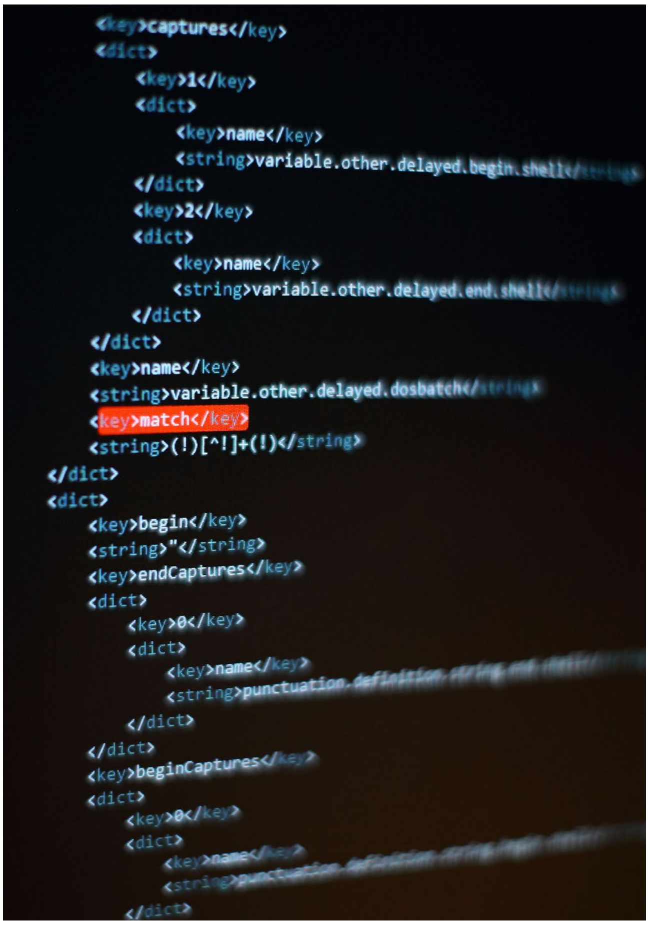
The CGI Analyse service makes use of the Triage solution and CGI's Phishing Analysts to rapidly investigate reported phishing threats. Once an email has been identified as malicious by the Analyse service, Vision can be used to find and remediate the entire phishing campaign, across the entire enterprise, within minutes.

Compliance

In order to help your organisation understand and remain in compliance Vision extensively audits and logs all actions. This allows you to understand who is searching for what within your environment. This is of great importance as these speedy searches no longer require privileged rights to the mail environment and provide transparency for all actions taken.

Non-malicious emails

Whilst Vision allows emails to quarantine with a single click, it also allows our team to seamlessly un-quarantine items if no threat is identified, returning them to your employee's inbox.



```
    <key>captures</key>
    <dict>
        <key>1</key>
        <dict>
            <key>name</key>
            <string>variable.other.delayed.begin.shell</string>
        </dict>
        <key>2</key>
        <dict>
            <key>name</key>
            <string>variable.other.delayed.end.shell</string>
        </dict>
    </dict>
    <key>name</key>
    <string>variable.other.delayed.dosbatch</string>
    <key>match</key>
    <string>(!)[^!]+(!)</string>
</dict>
<dict>
    <key>begin</key>
    <string>"</string>
    <key>endCaptures</key>
    <dict>
        <key>0</key>
        <dict>
            <key>name</key>
            <string>punctuation.definition.string.end.shell
        </dict>
    </dict>
    <key>beginCaptures</key>
    <dict>
        <key>0</key>
        <dict>
            <key>name</key>
            <string>punctuation.definition.string.begin.shell
        </dict>
```

CGI uses Vision software to search all employee inboxes, quickly removing and quarantining phishing emails.

Choose a service level that suits you

Your initial consultation with one of our cyber representatives will help you decide what level of service will best match your requirements and organisation's expectations.

Baseline:

- 1 template campaign pcm
- LMS (Learning Management System)
- Reporter button
- Monthly executive report

Enhanced:

- 2 campaigns (1 standard + 1 custom campaign pcm)
- LMS (Learning Management System)
- Reporter button
- Monthly executive summary template report including both campaigns
- Customisable landing pages

Advanced:

- 3 campaigns (1 standard + 1 customised + 1 targeted campaign pcm)
- LMS (Learning Management System)
- Reporter button
- Monthly executive summary template report including all three campaigns
- Customisable landing pages

Other options:

Triage:

- Reporter button
- Detection and response using Cofense Triage
- Cofense phishing intelligence repository
- Cofense AI automated tuning
- Executive monthly report including simulation if applicable

Vision:

- Automated malicious email discovery and removal
- Executive monthly report included with Triage

About CGI

Founded in 1976, CGI is among the largest IT and business consulting services firms in the world.

We are insights-driven and outcomes-based to help accelerate returns on your investments. Across 21 industries in 400 locations worldwide, our 82,000 professionals provide comprehensive, scalable and sustainable IT and business consulting services that are informed globally and delivered locally.

Our commitment: Insights you can act on.

For more information, visit cgi.com/uk/cyber-security
or email us at cyber.enquiry.uk@cgi.com