Cybersecurity in School

LGfL CyberCloud®

security.lgfl.net

LGfL CyberCloud®

security.lgfl.net

Sāgar Solanki

Cybersecurity Education Officer

Sāgar has worked in education for over 15 years, assuming various roles within Primary through to Further Education. Currently, he is responsible for providing cybersecurity solutions to LGfL schools. He also supports schools to comply with the DfE standards for cybersecurity in education.

LGfL CyberCloud®

security.lgfl.net

The presentation will look at:

- Rise in threats.
- What to know, and why it's important.
- How to stay secure.

(How LGfL can help you stay secure.)

LGfL CyberCloud®

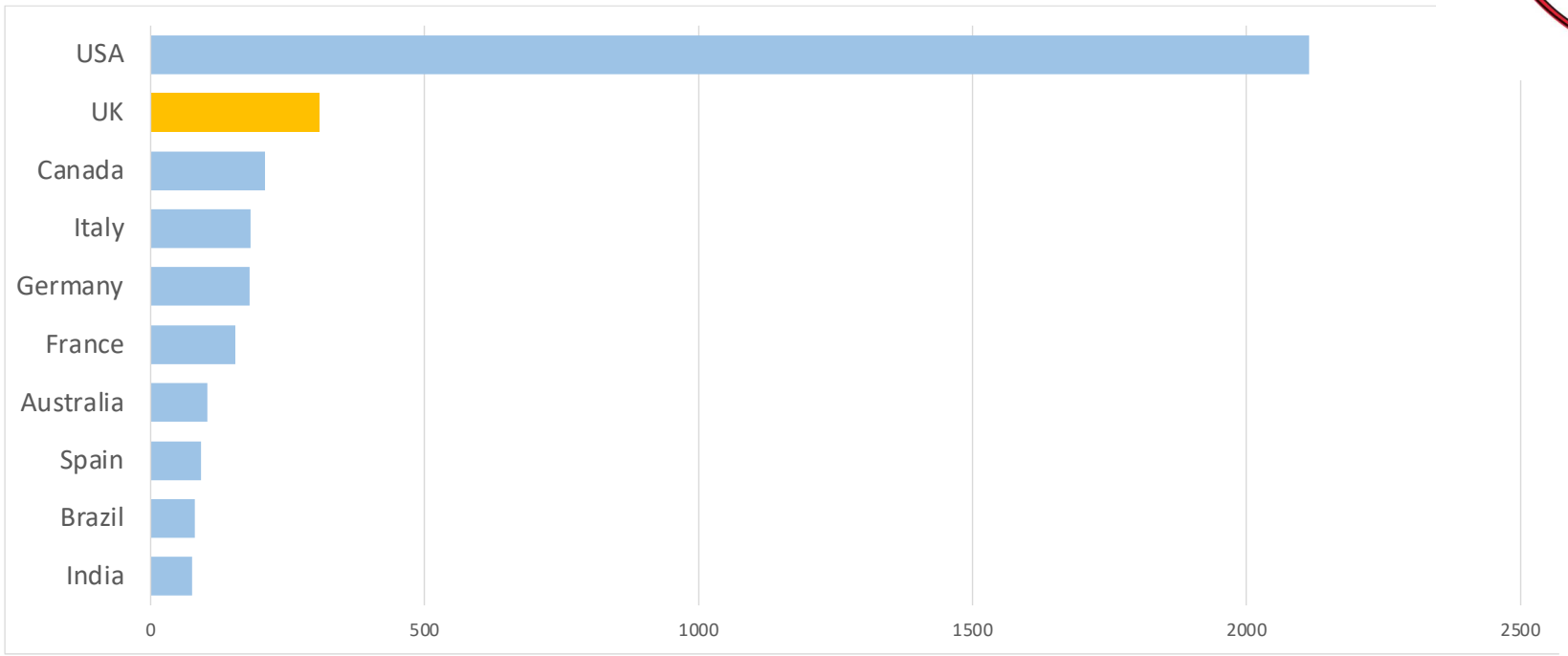
security.lgfl.net

Rise in threats.

LGfL CyberCloud®

security.lgfl.net

The UK is the second most attacked country



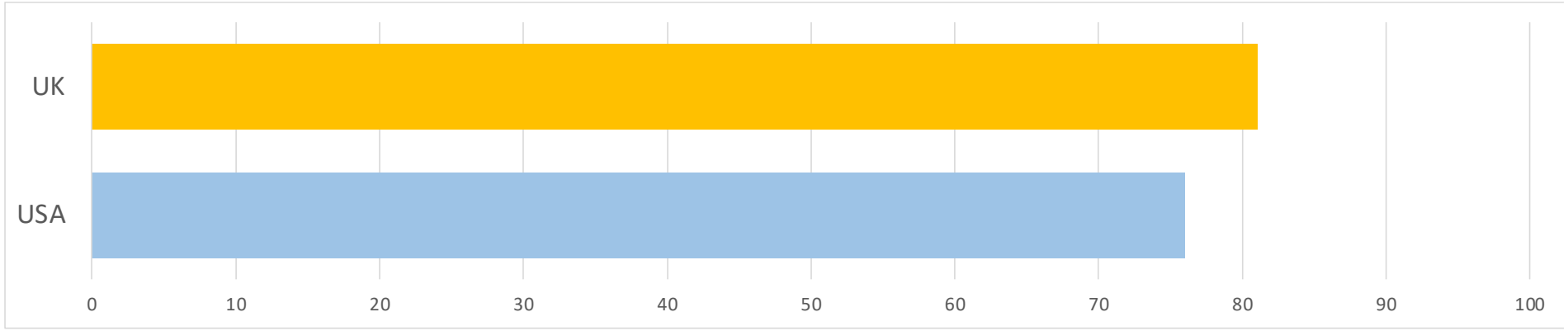
Top 10 countries by known ransomware attacks, Jan 2023 – Dec 2023

ThreatDown™
Powered by Malwarebytes

LGfL CyberCloud®

security.lgfl.net

When it comes to scale, the UK is attacked more than the USA



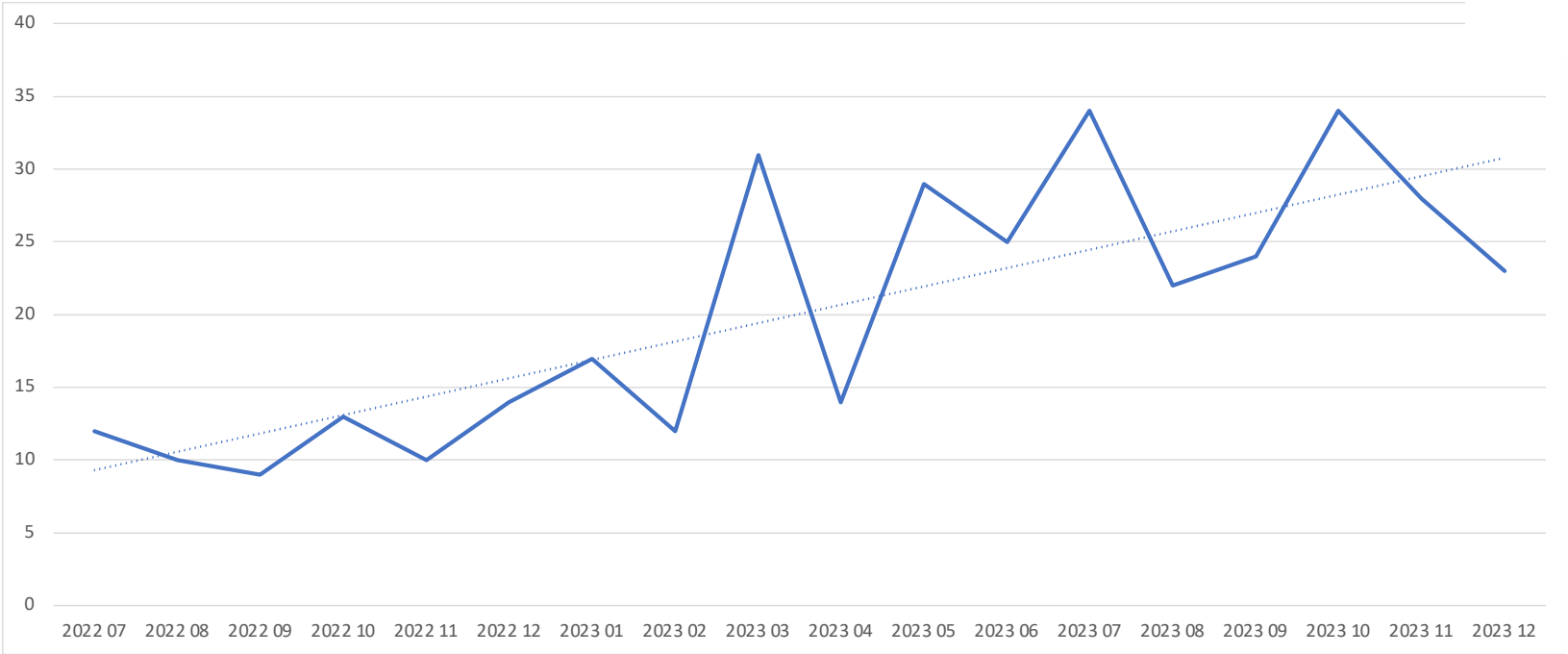
Known ransomware attacks per $1T GDP, Jan 2023 – Dec 2023

ThreatDown™
Powered by Malwarebytes

LGfL CyberCloud®

security.lgfl.net

Attacks are increasing



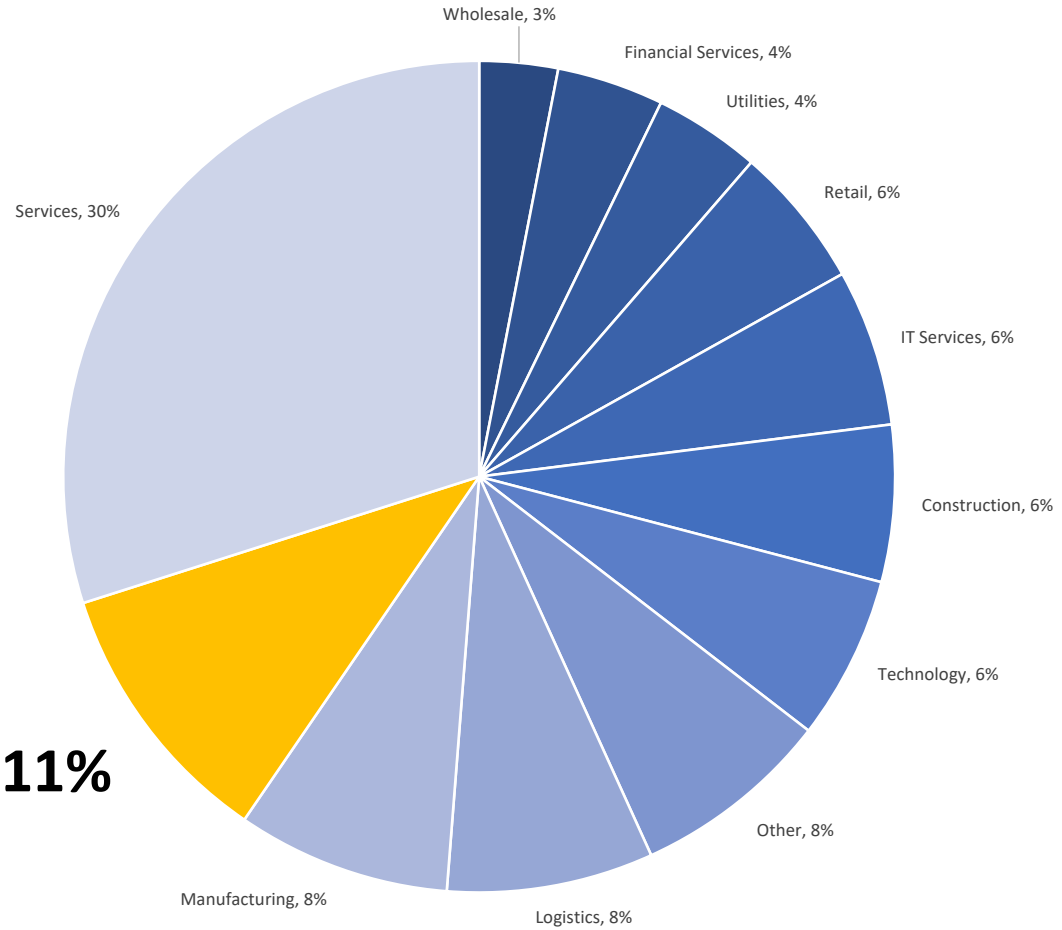
Known ransomware attacks in the UK Jul 2022 – Dec 2023

ThreatDown™ Powered by Malwarebytes

LGfL CyberCloud®

security.lgfl.net

Education is the second most attacked sector in the UK



Education 11%

Known ransomware attacks in the UK by industry sector Jul 2022 – Dec 2023

ThreatDown Powered by Malwarebytes

LGfL CyberCloud®

security.lgfl.net

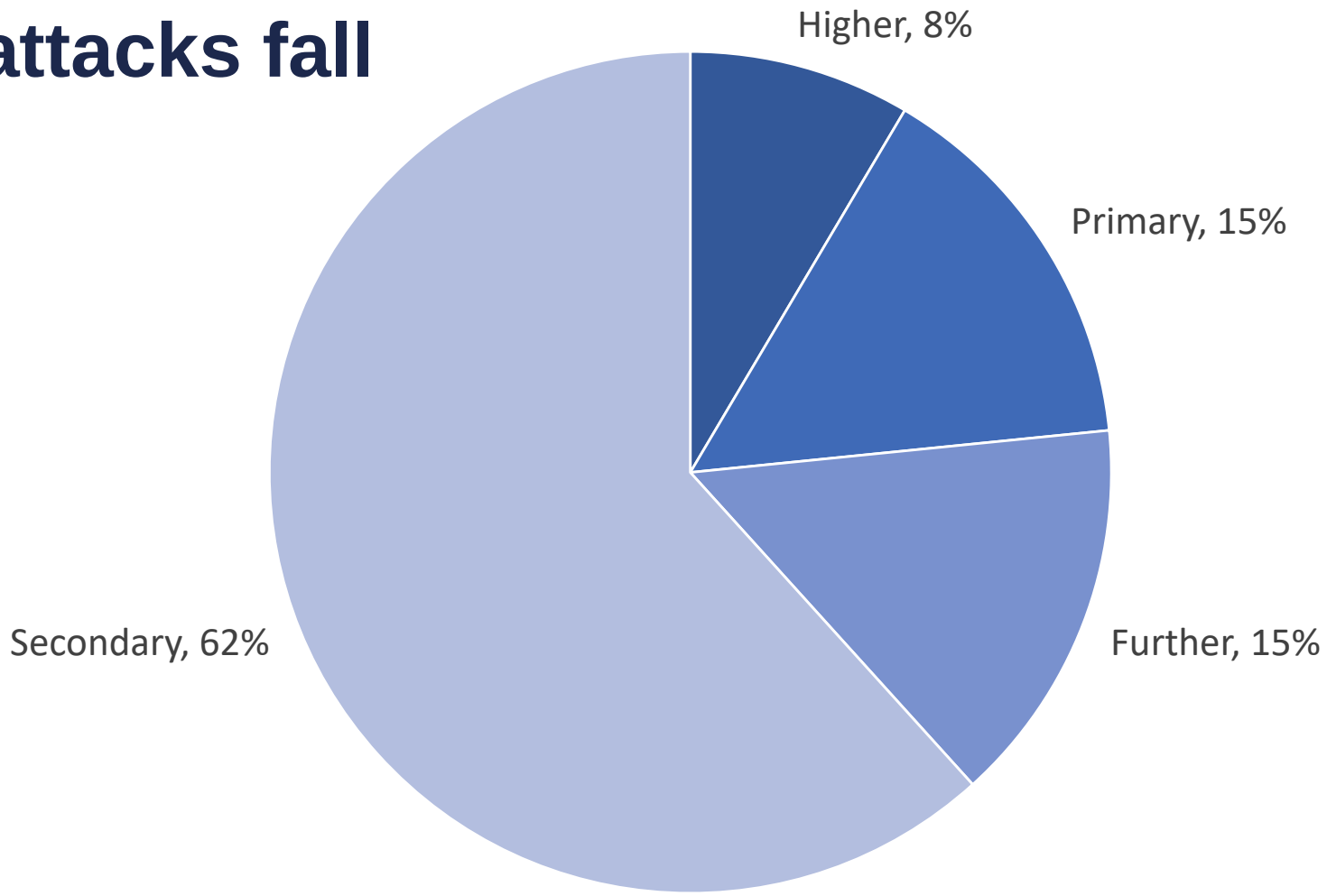
Education around the rest of the World seems to be doing better than the UK

Country	Education sector	
	% of total attacks	Rank among industry sectors
UK	11%	2nd
USA	8%	3rd
Germany	4%	10th
Canada	4%	10th
France	3%	12th
Italy	1%	15th
Japan	0%	N/A

Proportion of ransomware attacks in G7 countries affecting education, Jul 2022-Dec 2023

ThreatDown™ Powered by Malwarebytes

Where attacks fall



Known ransomware attacks on UK education by education tier, Jul 2022 – Dec 2023

LGfL CyberCloud®

security.lgfl.net

Why would they target my school?

LGfL CyberCloud®

security.lgfl.net

Schools carry out lots of **financial transactions**, which may only be signed off by a few members of staff.

Schools hold sensitive data on **pupils, parents and staff**.

A school's **support team are probably not security specialists**, with cybersecurity being only a small part of their day job.

Schools have **tighter budgets** and tend to have **older equipment** .

LGfL CyberCloud®

security.lgfl.net

Root Cause of Attack: Primary/Secondary Education

36%	29%	19%
Compromised Credentials	Exploited Vulnerability	Malicious Email
11%	4%	1%
Phishing	Brute Force Attack	Download

LGfL CyberCloud®

security.lgfl.net

36%

Compromised Credentials

How to protect against **compromised credentials** –

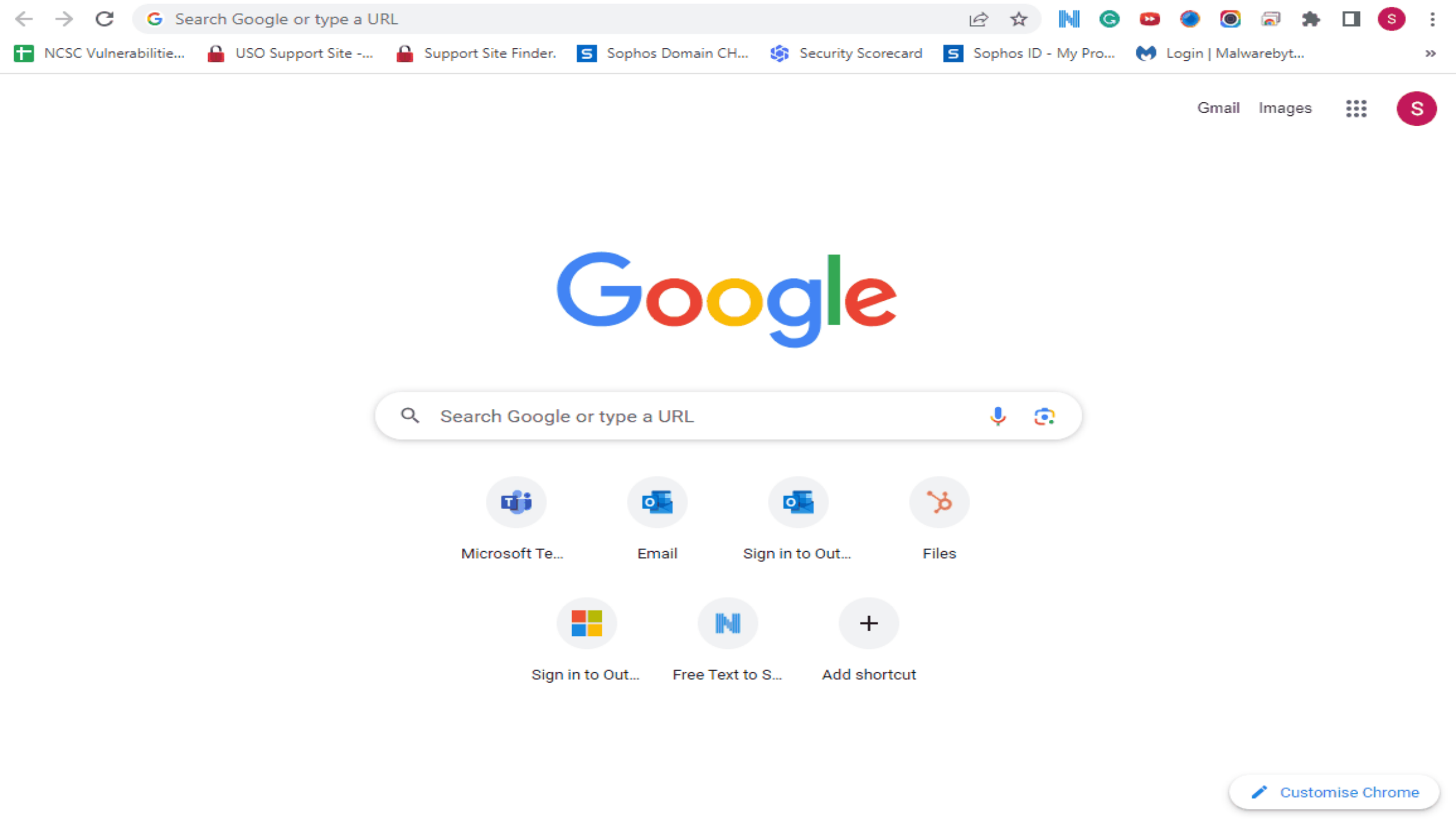
- MFA,
- HaveIBeenPwned,
- Password Manager (not reusing passwords).

LGfL CyberCloud®

security.lgfl.net

Using strong passwords

- Avoid commonly used passwords.
- Avoid passwords relating to personal information.
- Avoid passwords that have been breached previously.


Search Google or type a URL
NCSC Vulnerabilitie...
USO Support Site -...
Support Site Finder.
Sophos Domain CH...
Security Scorecard
Sophos ID - My Pro...
Login | Malwarebyt...
Gmail
Images
S
Google
Search Google or type a URL
Microsoft Te...
Email
Sign in to Out...
Files
Sign in to Out...
Free Text to S...
Add shortcut
Customise Chrome

LGfL CyberCloud®

security.lgfl.net

29%

Exploited Vulnerability

How to protect against **Exploited Vulnerabilities** –

- **SSR,**
- **VA Scans,**
- **NCSC EWS,**
- Patch Management,
- Keeping OS and Software that is supported/receiving updates.

LGfL CyberCloud®

security.lgfl.net

Security School Report

Example School

Generated **February 22, 2023**
by Cyber Cloud (cybercloud@lgfl.net), LGfL
Click Here to claim your scorecard and create your FREE account

LGfL CyberCloud®

A 93

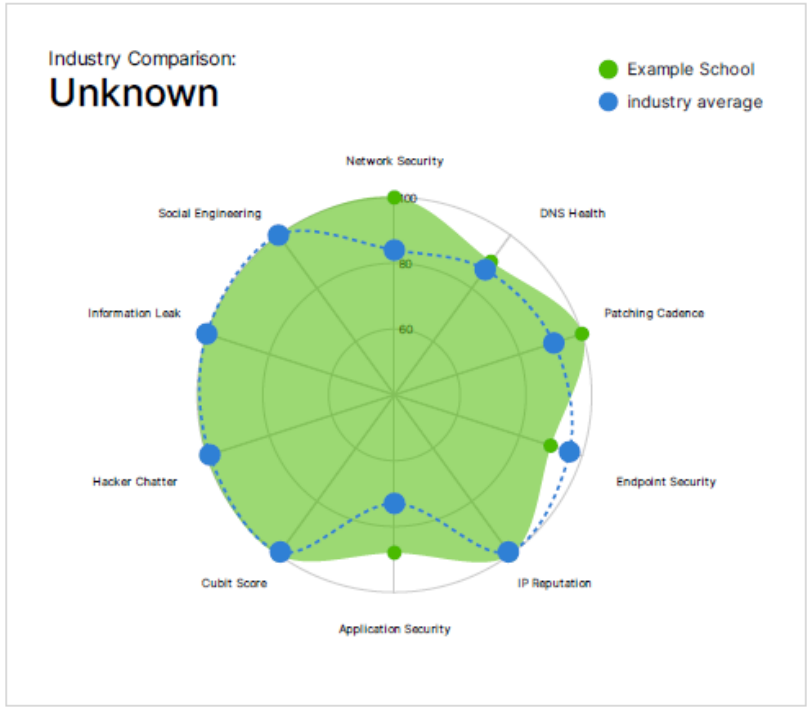
Threat Indicators

A 100 NETWORK SECURITY
Detecting insecure network settings

A 90 DNS HEALTH
Detecting DNS insecure configurations and vulnerabilities

A 100 PATCHING CADENCE
Out of date company assets which may contain vulnerabilities or risks

A 90 ENDPOINT SECURITY
Detecting unprotected endpoints or entry points of user tools, such as desktops, laptops, mobile devices, and virtual desktops



LGfL CyberCloud®

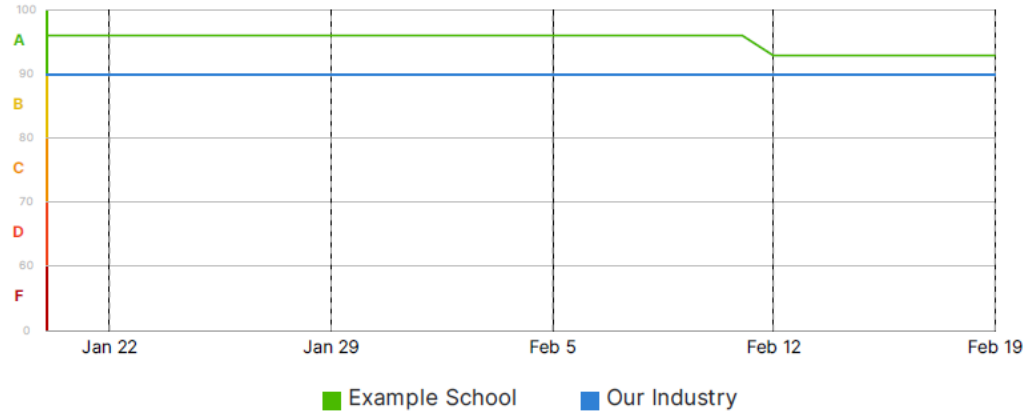
security.lgfl.net

Security School Report

A 100	**NETWORK SECURITY** Detecting insecure network settings	B 88	**APPLICATION SECURITY** Detecting common website applicatic vulnerabilities
A 90	**DNS HEALTH** Detecting DNS insecure configurations and vulnerabilities	A 100	**CUBIT SCORE** Proprietary algorithms checking for implementation of common security t practices
A 100	**PATCHING CADENCE** Out of date company assets which may contain vulnerabilities or risks	A 100	**HACKER CHATTER** Monitoring hacker sites for chatter a your company
A 90	**ENDPOINT SECURITY** Detecting unprotected endpoints or entry points of user tools, such as desktops, laptops, mobile devices, and virtual desktops	A 100	**INFORMATION LEAK** Potentially confidential company information which may have been inadvertently leaked
A 100	**IP REPUTATION** Detecting suspicious activity, such as malware or spam, within your company network	A 100	**SOCIAL ENGINEERING** Measuring company awareness to a s engineering or phishing attack

30-Day Score History

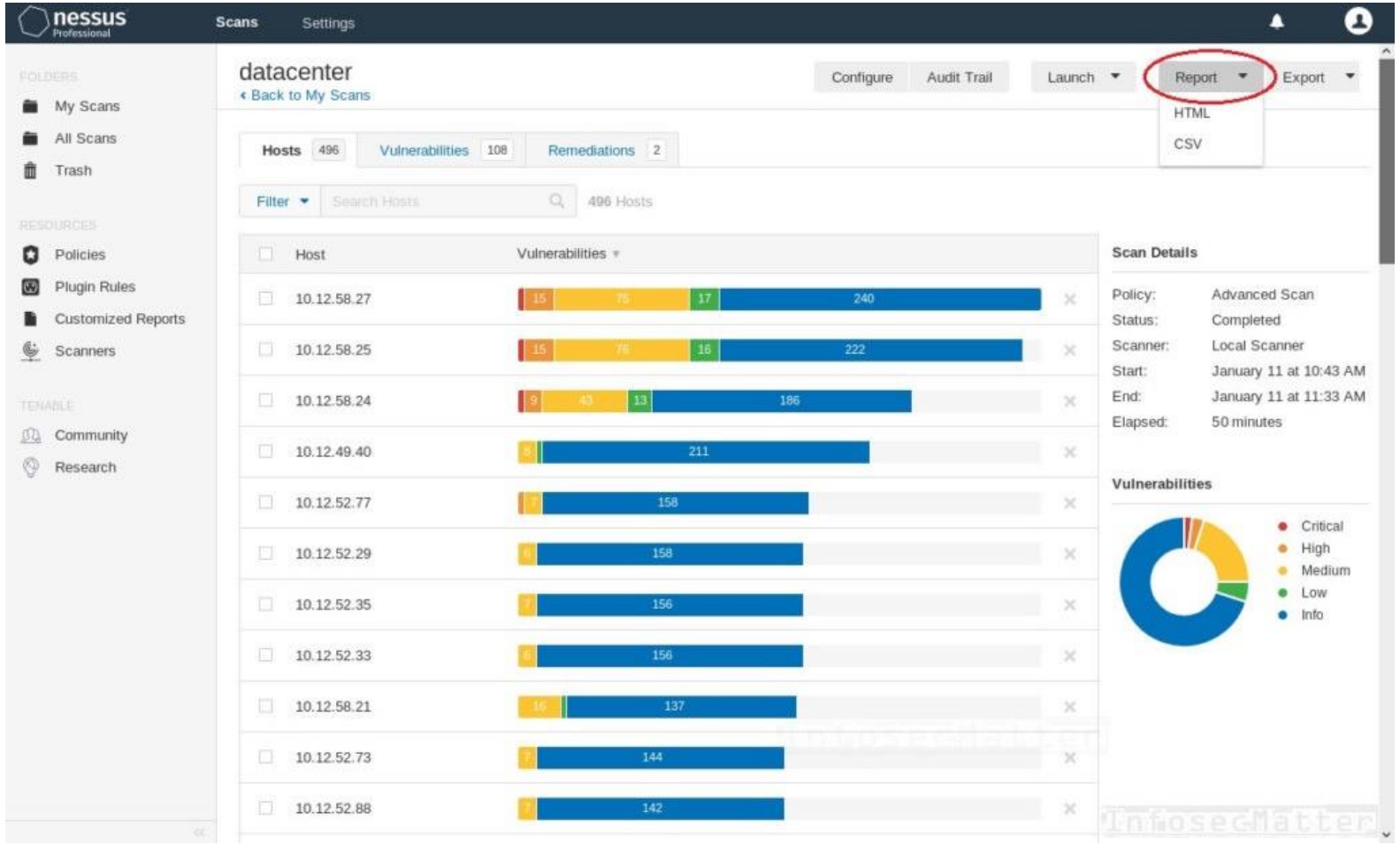
The chart below shows the evolution of the company's relative security ranking over time. Peaks in score performance represent improvements to overall security, remediation of open isues, and improved efforts to protect company infrastructure. Dips reflect introduction of system and application misconfigurations, prolonged malware activity.



LGfL CyberCloud®

security.lgfl.net

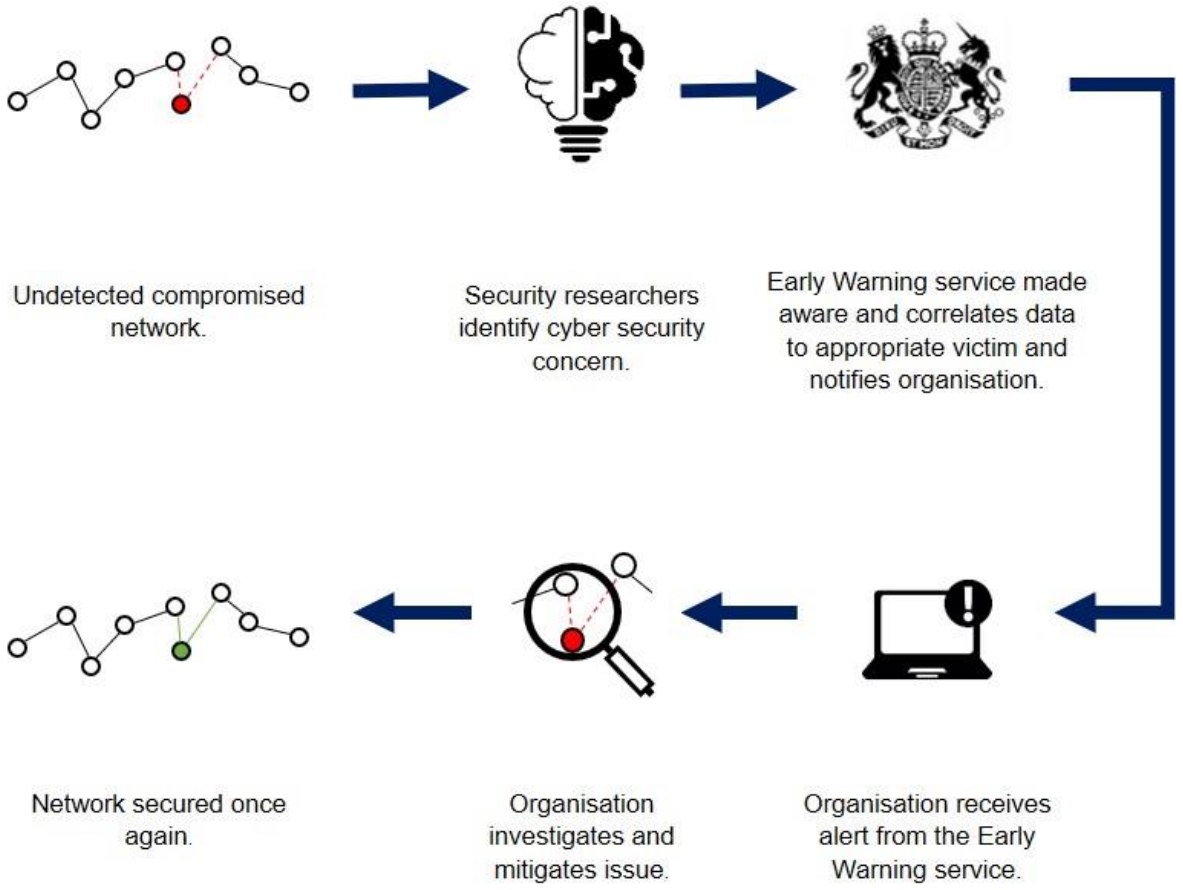
Vulnerability Scanning



LGfL CyberCloud®

security.lgfl.net

Early Warning Service



NCSC's new Early Warning service

designed to help organisations defend against cyber attacks by providing timely notifications about possible incidents and security issues

National Cyber Security Centre
a part of GCHQ

LGfL CyberCloud®

security.lgfl.net

19%

Malicious Email

How to protect against **Malicious Email**–

- SPF/DMARC/DKIM,
- Email scanning,
- **User awareness.**

LGfL CyberCloud®

security.lgfl.net

11%

Phishing

How to protect against **compromised credentials** –

- **Sophos Phish Threat,**
- **NCSC Training for School Staff.**

LGfL CyberCloud®

security.lgfl.net

Elizabeth sent you a new message

LM

LinkedIn Messaging <messaging-digest-noreply@linkedn.co>

To Gareth Jelley

Reply | Reply All | Forward | ...

Thu 15/07/2021 14:45

If there are problems with how this message is displayed, click here to view it in a web browser.

You have unread messages from **Elizabeth**

Elizabeth Mendez

Hi Gareth, I'm reaching out to see if you might be interested in a quick conversation. I was impressed by the skills and experience listed on your profile and...see more

Reply

Opportunity is always within reach. **Get the LinkedIn app.**

iOS . Android

Unsubscribe | Help

You are receiving Messages from connections digest emails.

Ph Sophos Phish Threat

Ideal behavior	**0%** reported the email without being caught
Good behavior	**0%** caught but reported the email
Neutral behavior	**0%** never opened the email
Not ideal behavior	**75%** opened the email but did not report it
Risky behavior	**25%** caught and did not report it

LGfL CyberCloud®

security.lgfl.net

4%

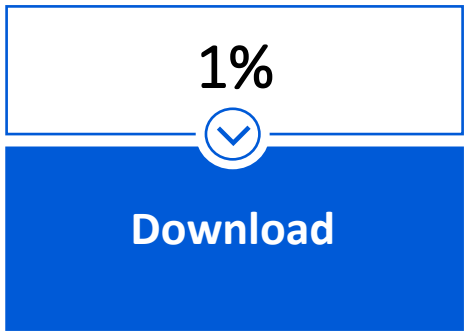
Brute Force Attack

How to protect against **compromised credentials** –

- Not using common/obvious passwords,
- Auto lockout after failed attempts (careful not to make this a game the pupils play on teachers)

LGfL CyberCloud®

security.lgfl.net



How to protect against **compromised credentials** –

- Download – AV

LGfL CyberCloud®

security.lgfl.net

SOPHOS Dashboards My Products Threat Analysis Center Alerts Reports More

Anne Example School

Sophos Central Dashboard

See a snapshot of your security protection

1	0	1	0
Total Alerts	High Alerts	Medium Alerts	Low Alerts

Most Recent Alerts

View all Alerts

⚠	Apr 11, 2024 3:25 PM	Device is not encrypted.	Sagar-Sophos-V...	Sagar-Sophos-VM	Show full details

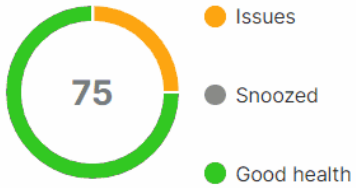
Device is not encrypted.

Health summary

Go to Account Health Check

Show scores for organizations with a similar number of devices: 1-49

Your overall health score



Health check scores

Protection installed	100	Tamper protection	75
Other organizations	88	Other organizations	84

LGfL CyberCloud®

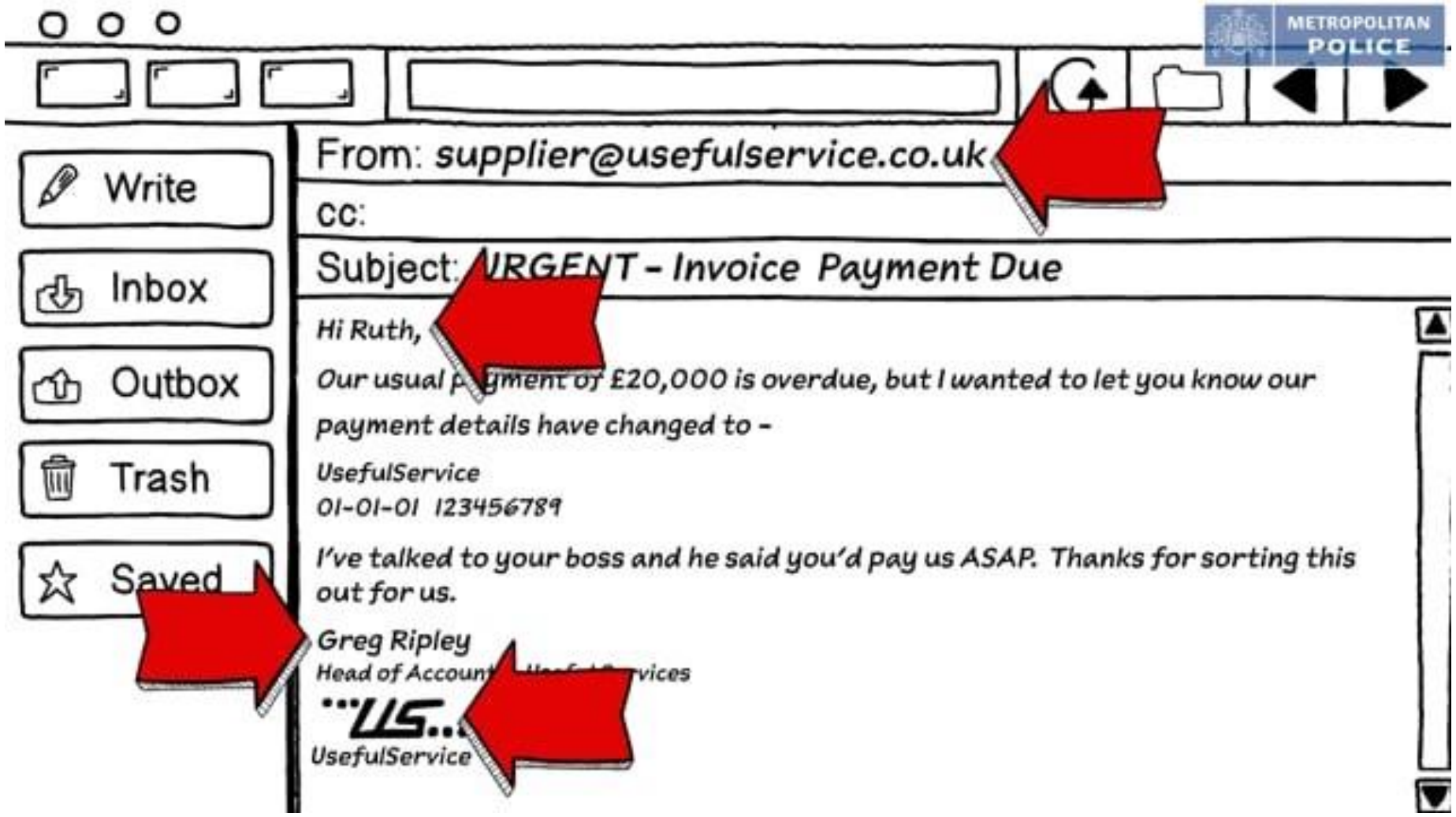
security.lgfl.net

Who is behind cyber attacks?

- Criminals that might wish to target your school for financial gain.
- Criminals that have identified a potential weakness in the school's technology or processes.
- Staff or pupils that could be responsible for attacks either intentionally or accidentally.

LGfL CyberCloud®

security.lgfl.net



LGfL CyberCloud®

elevate.lgfl.net

National Cyber Security Centre
a part of GCHQ

School hacked by pupil broke Data Protection Act

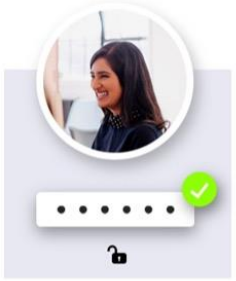
Case Study - Password management

LGfL CyberCloud®

elevate.lgfl.net

Case Study – Password management

School hacked by pupil Broke Data Protection Act



Accessed school MIS → Used teacher's password → 20,000 records involved → Duplicate passwords used → Disciplined by ICO

LGfL CyberCloud®

elevate.lgfl.net

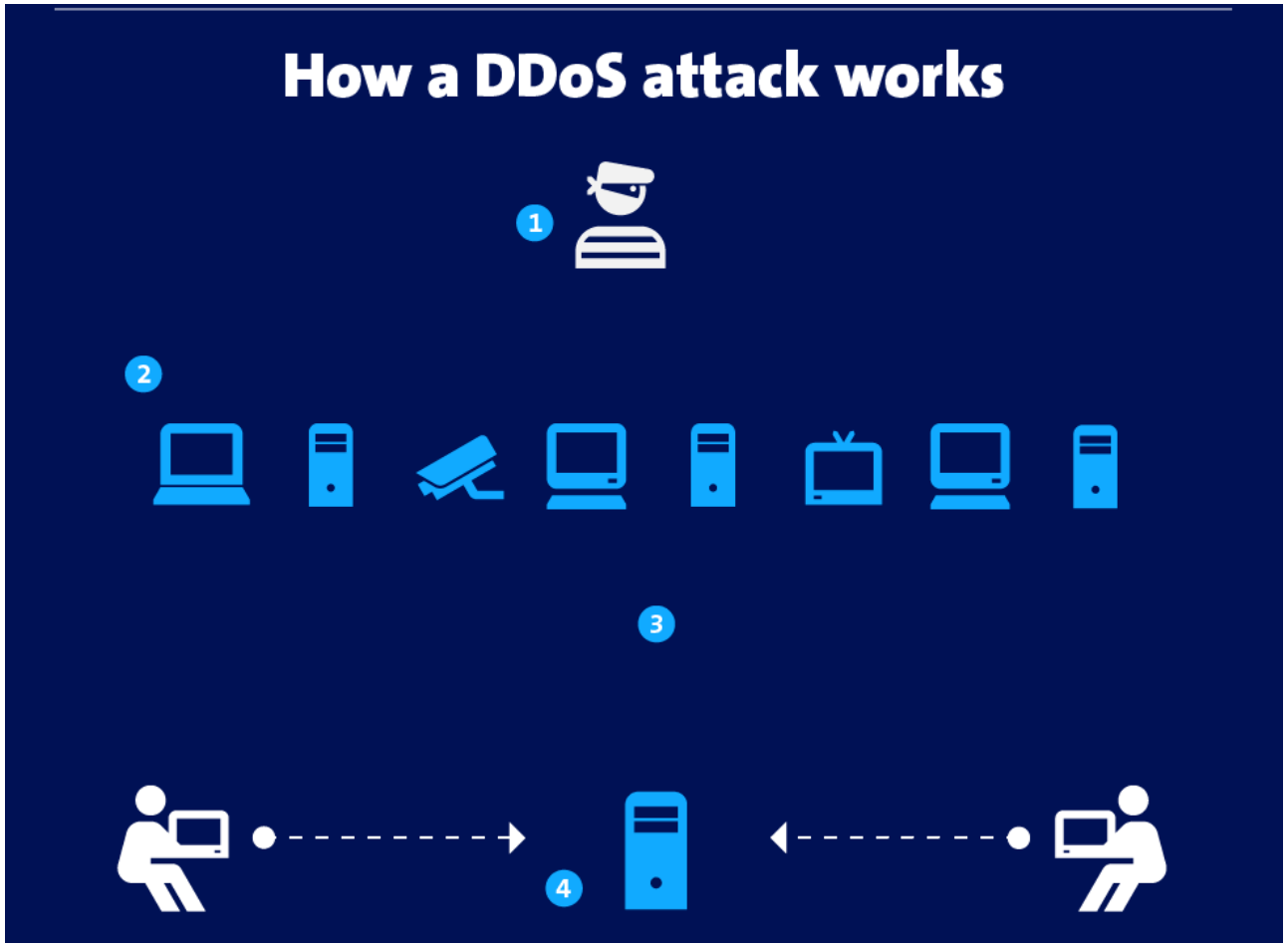
CYBER CHOICES

LGfL CyberCloud®

elevate.lgfl.net

DDos (Distributed denial of Service) – What is it?

Denial of Service occurs when a website can't handle its normal traffic, sometimes unintentionally. However, a **Denial-of-Service Attack** is intentional, where the attacker aims to overload the server and make it unavailable to users.



Ref: chemicloud.com/kb/article/what-is-a-ddos-attack/

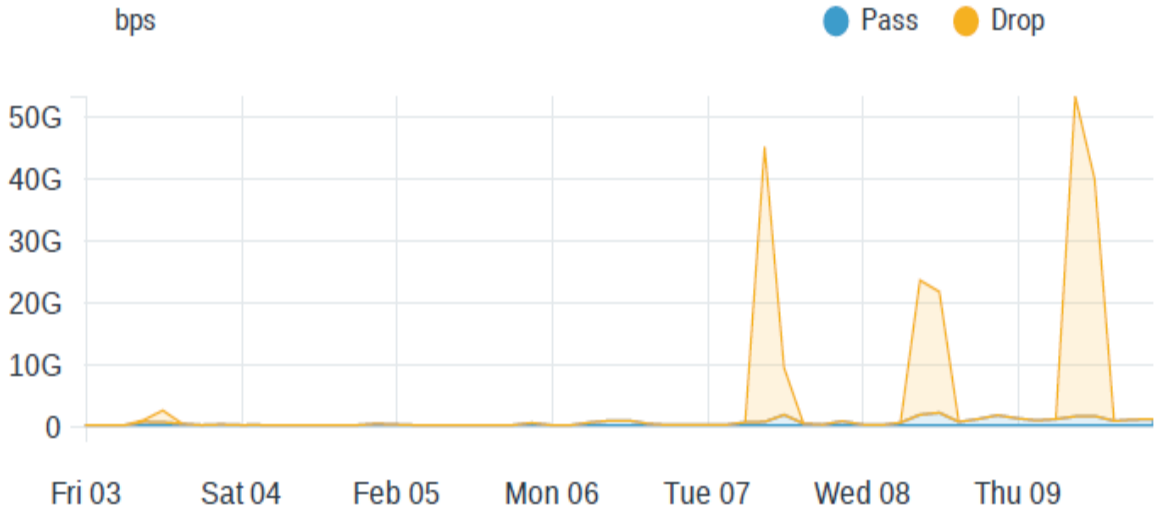
LGfL CyberCloud®

security.lgfl.net

LGfL CyberCloud®

security.lgfl.net

DDoS Protection



DDoS attacks detected against LGfL:

- **over the last 12 months: 48**
- **since 1st January 2023: 42**

Summary | DDoS | Traffic Trends | AIF Standard Feed | AIF Threat Indicator Feed

Largest or most significant DDoS attacks around the world over the last 24 hours involving ISPs participating in ATLAS.

Carrier	Time	Attack
3035 *No Self-Classification*	02/07/23 19:01:01 7 mins.	**DDoS Total Traffic** 46.55 Mpps,10.81 Gbps Src: 0.0.0.0/0,103.234.22.105/32,36.35.16.160/32,101.132 DST: xx.xx.102.190/32 Port(s): 22,37030,38666,38672,38674,38676,38680,38686
891 tier2 in none_region	02/08/23 07:26:36 18 mins.	**DDoS IP Fragmentation** 41.45 Mpps,62.45 Gbps Src: 0.0.0.0/0,198.98.48.0/20,45.0.0.0/9,209.141.56.0/21,2 DST: xx.xx.156.181/32 Port(s): 7,53,80,111,123,137-138,161,177,253,389,427,500
3518 *No Self-Classification*	02/07/23 10:06:45 2:07	**DDoS IP Fragmentation** 38.27 Mpps,20.07 Gbps Src: DST: Port(s):
4239 *No Self-Classification*	02/07/23 20:20:14 42 mins.	**DDoS Total Traffic** 36.37 Mpps,9.61 Gbps Src: DST: Port(s):
3518 *No Self-Classification*	02/07/23 10:24:14 58 mins.	**DDoS flood** 34.20 Mpps,14.01 Gbps Src: DST: Port(s):

LGfL CyberCloud®

elevate.lgfl.net

How to stay safe?

LGfL CyberCloud®

security.lgfl.net

Defend against phishing attempts.

Image: https://www.forbes.com/sites/technology/article/what-is-phishing/

LGfL CyberCloud®

security.lgfl.net

How do I defend myself against phishing attempts?

1. Reduce the information available to attackers.
2. Know the influence techniques.
3. Know what ‘normal’ looks like.
4. Don’t be embarrassed to ask for help.
5. Report if you click!

LGfL CyberCloud®

security.lgfl.net

Phishing example

Subject: **URGENT - Email capacity - you will soon stop receiving emails**

AD **admin@m1cr0s0ftlogin.org**

Weds 05/02/2020 16:16

To: businessmanager@theacademy.sch.uk

Dear businessmanager,

You have reached the size limit for your mailbox and you will shortly stop receiving emails until you have confirmed that you require more space.

Please click here to confirm your email login and password to increase your capacity and continue to receive emails.

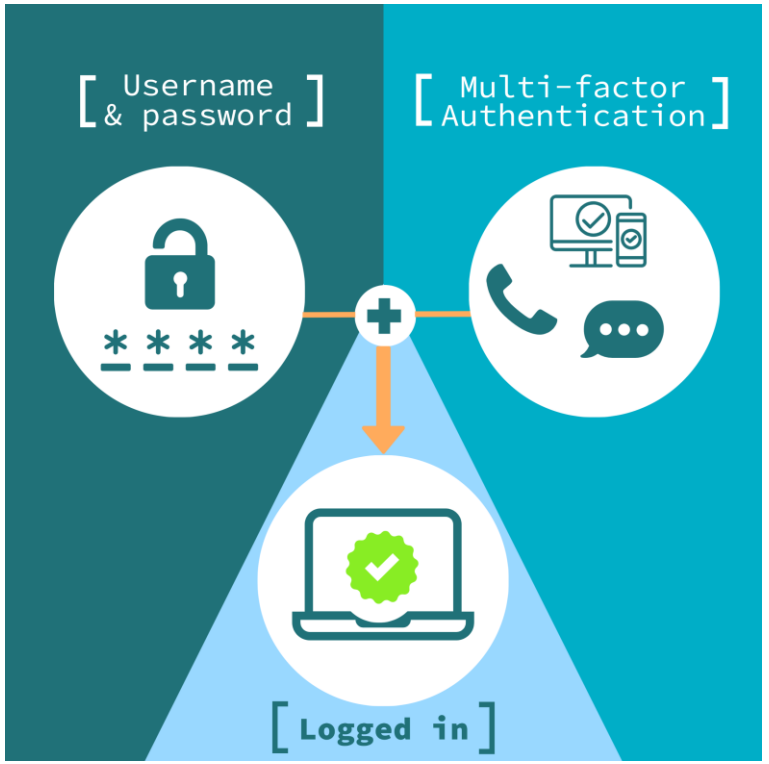
Kind regards, www[.]M1cr0s0ftlogin[.]org

Microsoft

LGfL CyberCloud®

security.lgfl.net

Use strong passwords



LGfL CyberCloud®

security.lgfl.net

Secure your devices

1. Do not ignore updates.
2. Only download apps from trustworthy sources.
3. Physically protect your device.
4. If you need to use USB storage, ensure it is encrypted. (Online Storage Google Space/One Drive.) Do not encourage USB.

LGfL CyberCloud®

security.lgfl.net

If in doubt call it out.

1. Report any suspicious activity.
2. Report as soon as possible.
3. Don’t be afraid to challenge.

LGfL CyberCloud®

elevate.lgfl.net

Thank you.

LGfL CyberCloud®

security.lgfl.net

Thank you

Questions?

Twitter:	@lgflcybercloud
Portal:	security.lgfl.net
Newsletter:	newsletter.lgfl.net
Email:	cybercloud@lgfl.net