

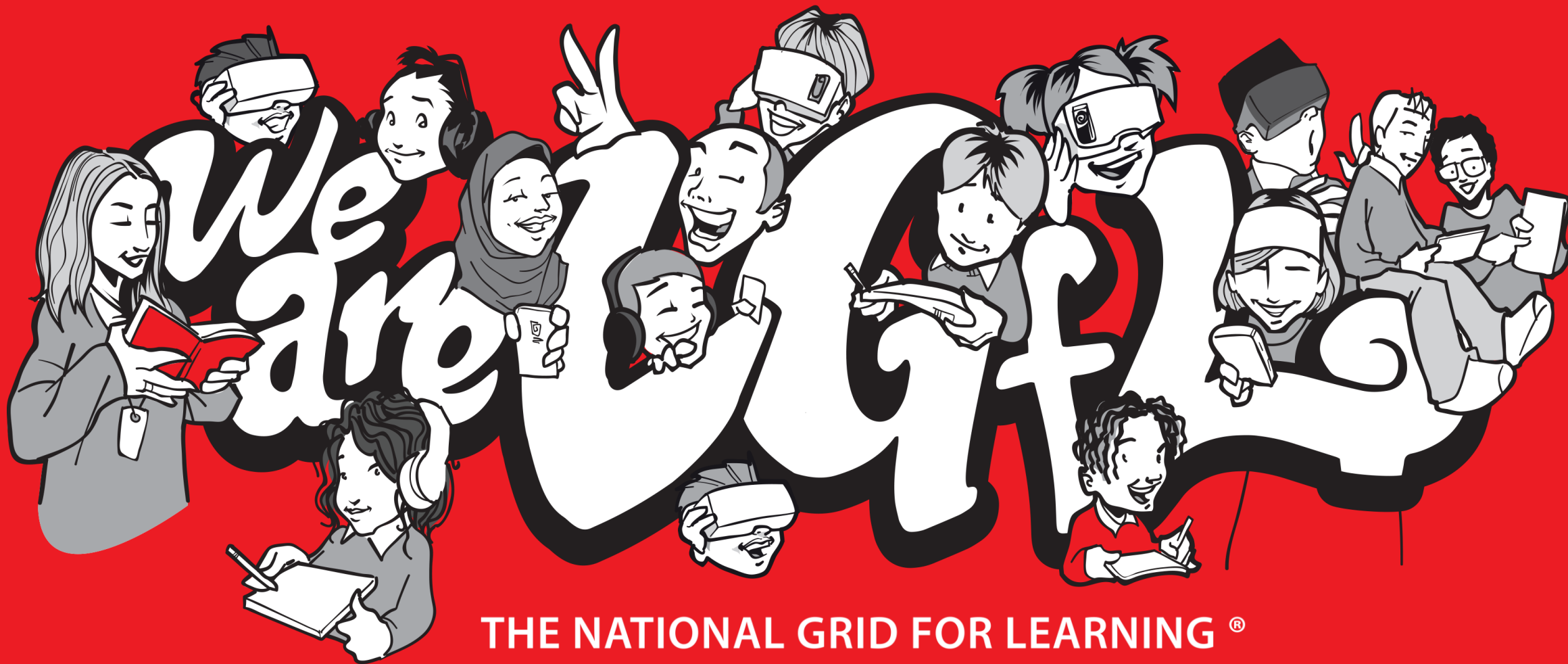
# Schools Don't Wanna Cry

Mark Bentley, Safeguarding & Cybersecurity Manager, LGfL



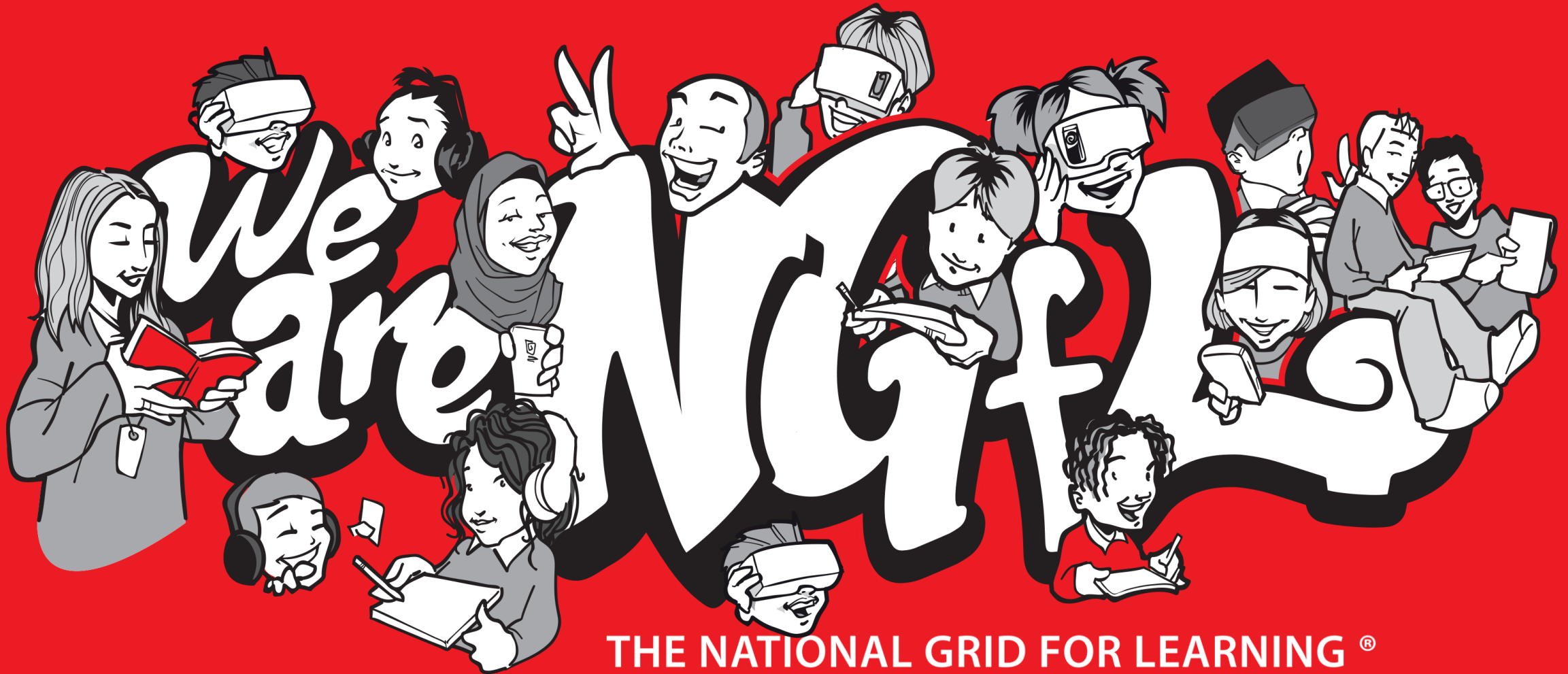
LGfL

CyberCloud



THE NATIONAL GRID FOR LEARNING®





THE NATIONAL GRID FOR LEARNING®

# SAVE MORE THAN YOU SPEND & KEEP CHILDREN SAFE

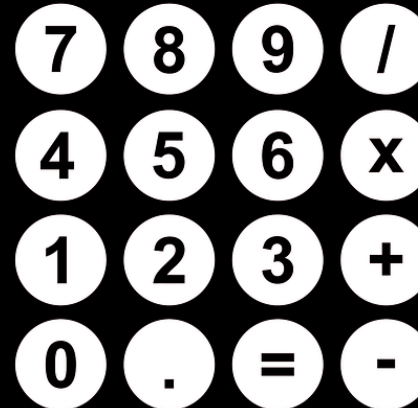
**PLEDGE  
2020**

Free Boost  
to Your  
Bandwidth



**LGfL**

SAVINGS  
CALCULATOR



DigiSafe

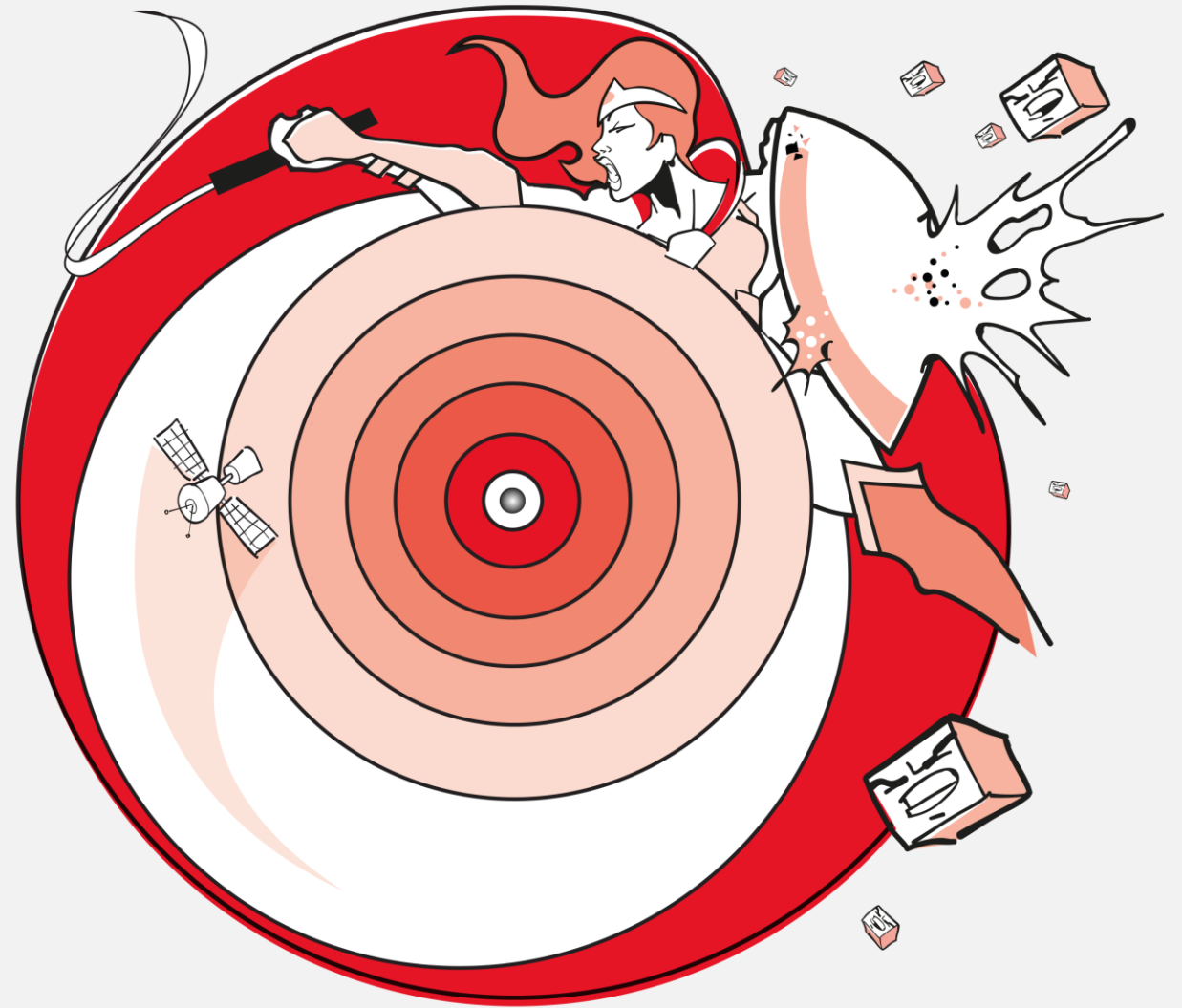
*Keeping children safe*



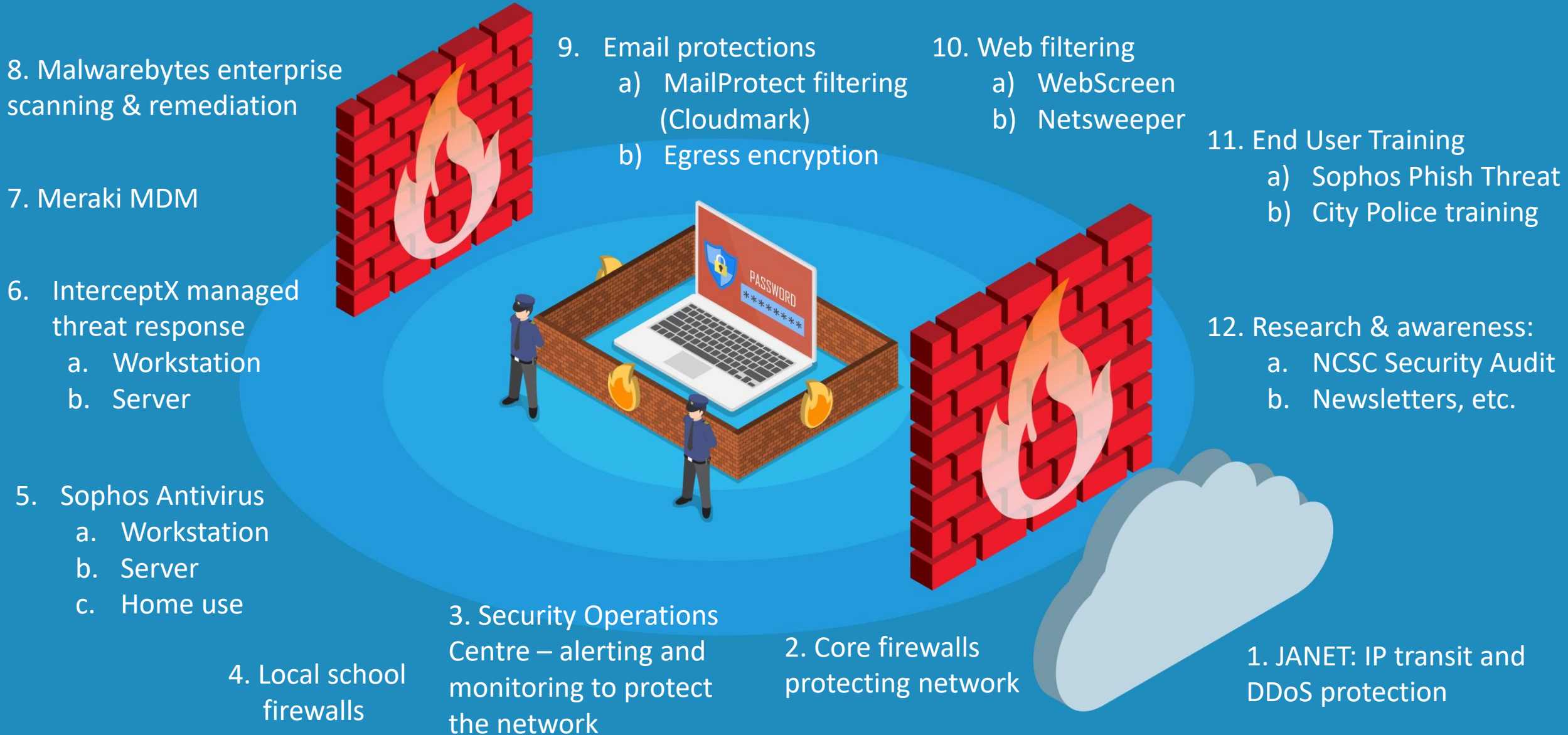
CyberCloud

*Keeping schools secure*

Shielding schools  
from cyberthreats  
with **LGfL** CyberCloud<sup>®</sup>



# Twelve Layers of Defence from **LGfL** CyberCloud®

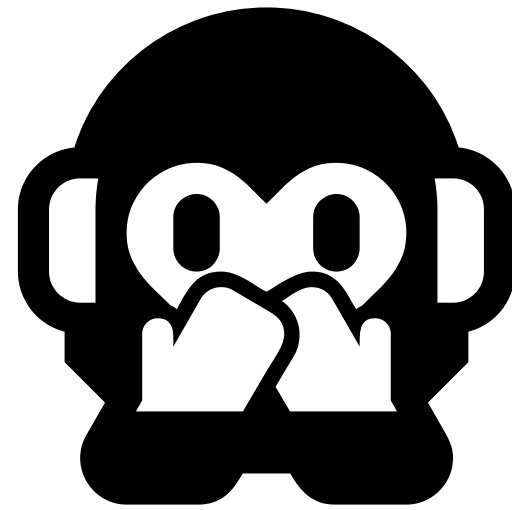
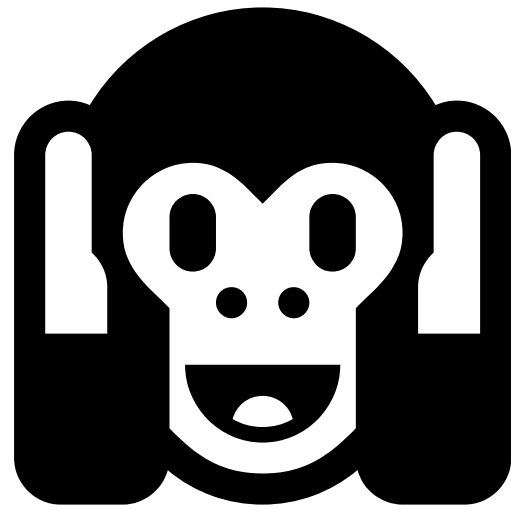








# The problem/s with cybersecurity





Wow, this is boring.



Not my area.

## GCSE coursework lost in cyber attack on Bridport school

© 13 March 2019 [f](#) [m](#) [t](#) [e](#) [Share](#)



The Sir John Colfox Academy has about 1,000 pupils

Hackers have used ransomware to encrypt files at a school, causing it to lose some students' GCSE coursework.

## Schools lose £145k to fraudsters, figures show

EB News: 02/03/2018 - 11:02



[t](#) [f](#) [in](#) [e](#)

Fraudsters posing as headteachers have conned schools across the country out of tens of thousands of pounds since last September.

As reported by Schools Week, figures from the National Fraud Intelligence Bureau show that since last September, 48 schools have reported the scam, most of them in December and January.

Of those, 12 schools lost out on £145,124 between them.

Latest Magazine  
**Education Business**  
THE BEST APPROACH TO SCHOOL DESIGN  
Latest Features  
Inspiring greatness in young people  
Understanding modular buildings  
The pathway to a STEM career  
Making the case for sprinklers in schools  
What can school leaders do to develop resilience?

## Newcastle school targeted in fees phishing scam

© 20 January 2019 [f](#) [m](#) [t](#) [e](#) [Share](#)



Royal Grammar School in Newcastle was one of a number of schools targeted in the cyber attack

Fee-paying schools were targeted in a cyber attack which accessed parents' email addresses, it has emerged.



# NEWS

Home | UK | World | Business | Politics | Tech | Science | Health | Family & Education

EWS | FABULOUS | MONEY | MOTORS | TRAVEL | TECH | DEAR DEIDRE | PUZZLES | VOUCHERS

All Tech | Science | Phones & Gadgets | Gaming

## PAY TO PLAY TikTok stars 'exploiting kids' for gifts as Brit fans pay £100s just to talk to them

REVEALED

Sean Keach, Digital Technology and Science Editor  
3 Jul 2019, 10:27 | Updated: 3 Jul 2019, 10:30

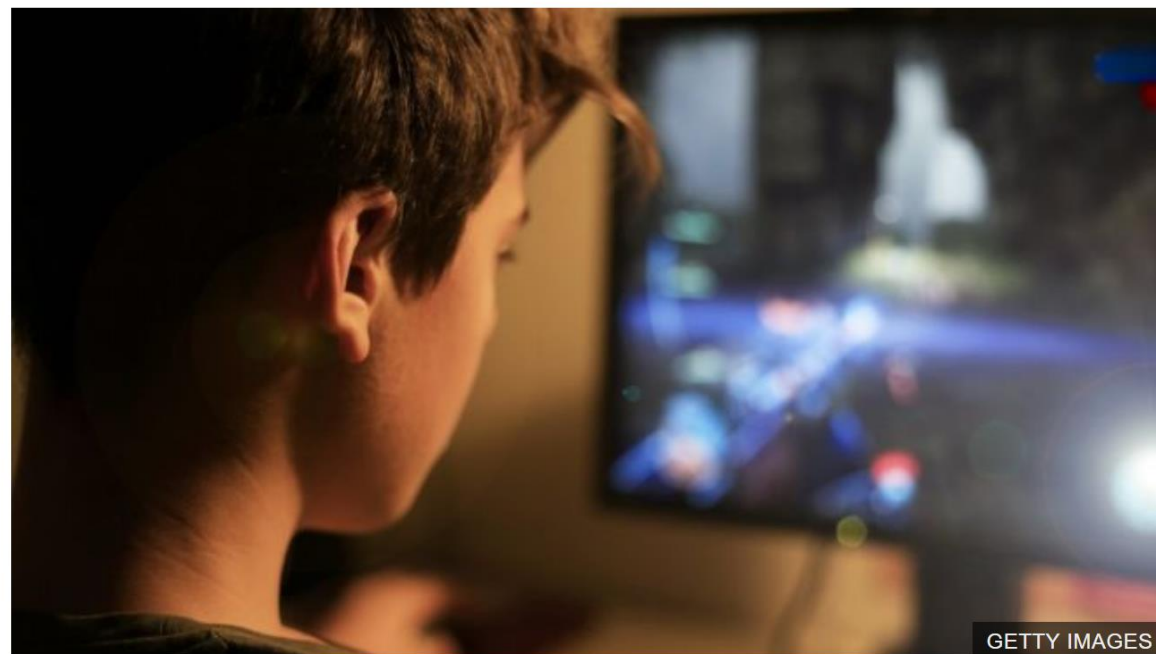


## 'My son spent £3,160 in one game'

By Zoe Kleinman  
Technology reporter, BBC News

15 July 2019

Share



ANALYZE

Dashboard

Reports

MANAGE

People

Campaigns

CONFIGURE

Settings

## Choose Training

Training is a great way to increase security knowledge among your users and reduce the risk to your organization.


- Phish Threat training (recommended)**  
Automatically enroll caught users in Sophos training content
- Use my own training**  
Automatically redirect caught users to your own hosted content
- No training**  
Redirect caught users to a fake 404 page (good for baseline assessments)

### Training reminders

- Send daily reminder emails until training is complete**

Search  All Trainings

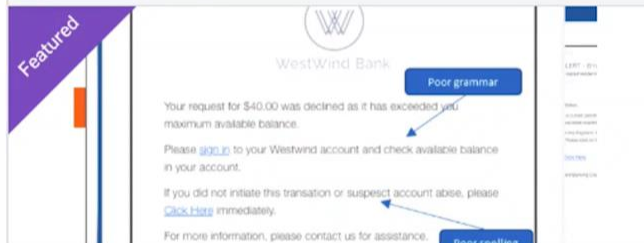
**Basic Phishing Tips Interactive** 2 Min



Choose this training

The card features a purple 'Featured' banner in the top-left corner. The main image shows a red fishhook with a red fish inside, set against a dark blue background. Text reads 'WOAH! You just got phished!' and 'This wasn't a real attack, but it could have been!'.


**Intro To Phishing** 2 Min



Choose this training

The card features a purple 'Featured' banner in the top-left corner. The main image shows a screenshot of a WestWind Bank email with annotations: 'Poor grammar' pointing to a typo and 'Poor spelling' pointing to a misspelled word. Text on the card includes: 'Your request for \$40.00 was declined as it has exceeded your maximum available balance. Please log in to your Westwind account and check available balance in your account. If you did not initiate this transaction or suspect account abuse, please Click Here immediately. For more information, please contact us for assistance.'

**PII Interactive** 10 Min



Choose this training

The card features a purple 'Featured' banner in the top-left corner. The main image shows a person's profile on a screen with a bright yellow sunburst effect behind the name 'John Doe', illustrating Personally Identifiable Information (PII).

**Phishing Attacks Overview** 6 Min



Choose this training

The card features a purple 'Featured' banner in the top-left corner. The main image is a cartoon illustration of a hacker in a mask and hood holding a laptop, with a question mark above a confused-looking man. Both are holding signs that say 'www.bankofamerica.com'.

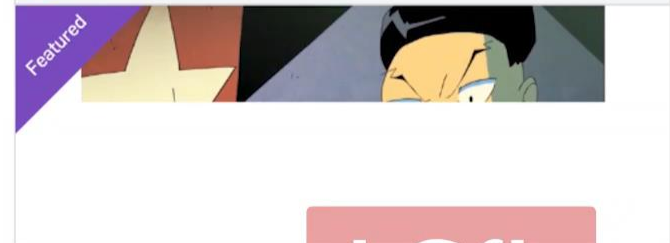
**Phishing Interactive** 7 Min



Choose this training

The card features a purple 'Featured' banner in the top-left corner. The main image shows a computer monitor with an envelope icon on the screen, surrounded by various icons representing security and communication.

**Spear Phishing** 4 Min



Choose this training

The card features a purple 'Featured' banner in the top-left corner. The main image shows a close-up of a person's face looking at a screen, with a large red 'LGfL' watermark in the bottom right corner.

**Targeted Phishing** 5 Min

**Ten Ways To Spot A Phish** 2 Min

**2-Factor Account Takeover** 4 Min

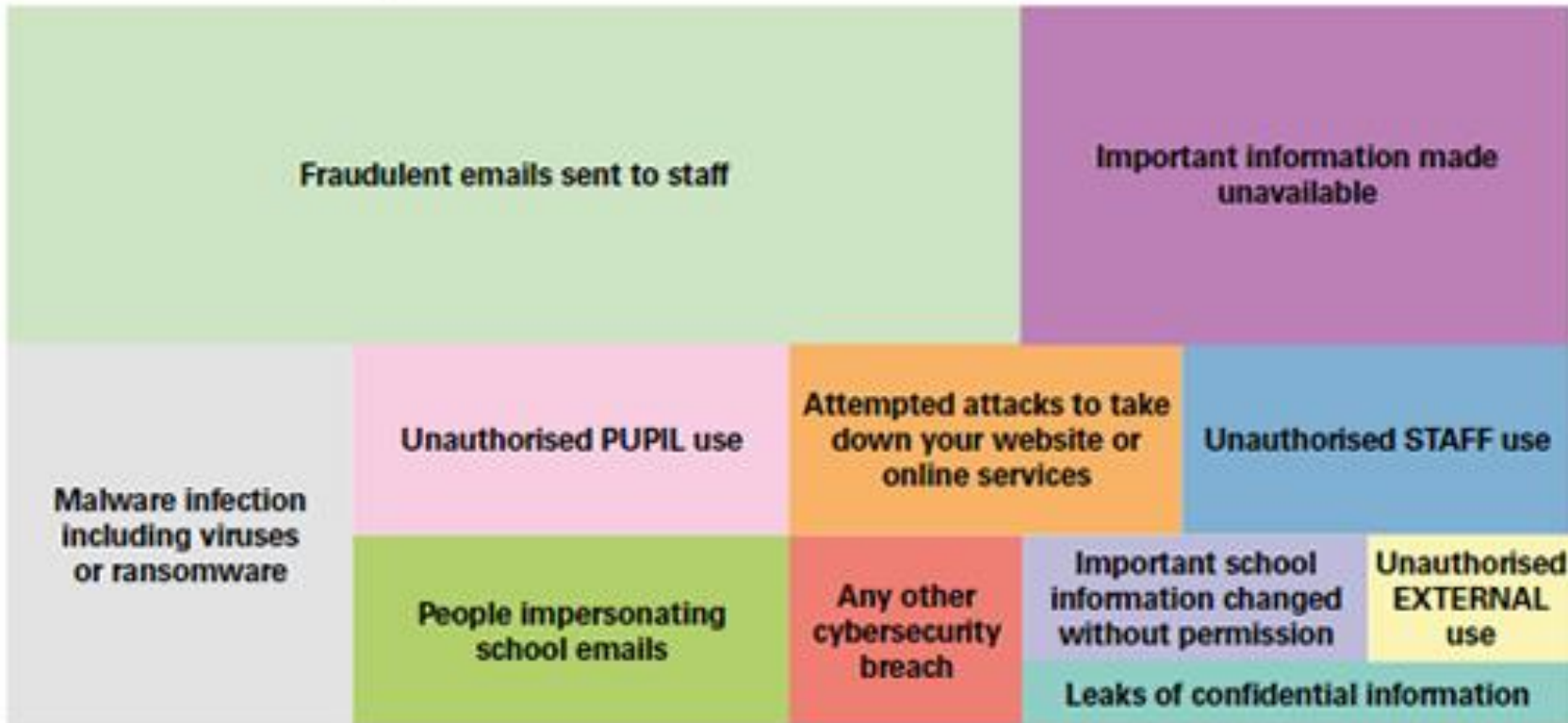


[securityaudit.lgfl.net](https://securityaudit.lgfl.net)



## HAVE YOU EVER...?

As far as you know, have you experienced the following?  
(% of 432 schools answering yes)



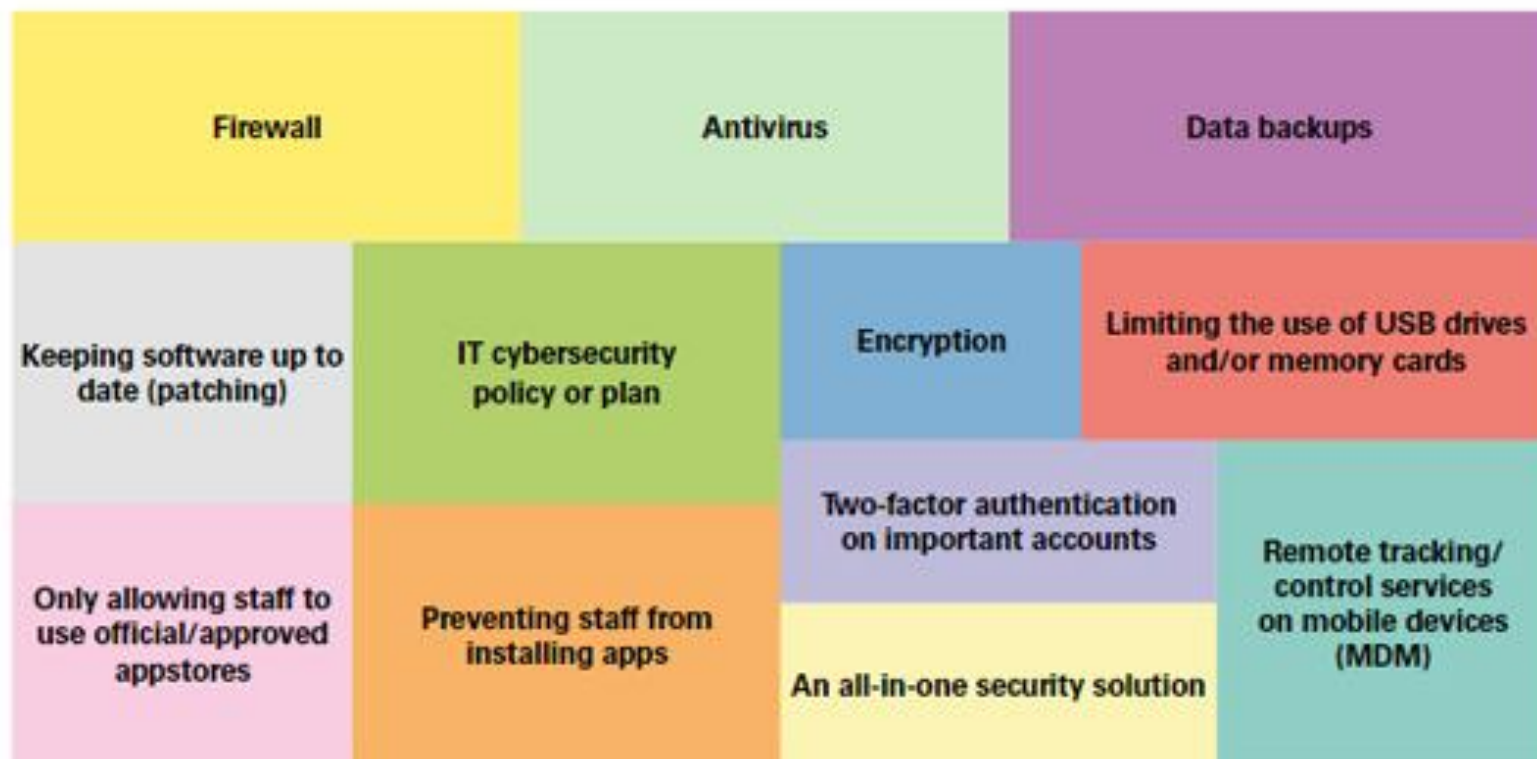
According to Malwarebytes CEO Marcin Kleczynski, **“Our experiences suggest that many schools may be unaware that they are infected; with the amount of malware that can fly ‘under the radar’, it’s possible this number could be much higher in reality.”**

According to Mark Weir, Director UK&I / EMEAR Cyber Security at leading firewall manufacturer Cisco,

**“sadly, education is a target for the criminal community with many examples being reported of schools being attacked, with cyber criminals trying to gain access to student data or important research. These actors try and blackmail the school or user by threatening to share this sensitive information.**

## CYBERPREPARED – IMMATURITY OR SECURITY?

Do you have the following security measures in place in your school?  
(% of 432 schools answering yes)





Do you have a business continuity plan in place?  
% of 432 schools

## Don't be a circle short of a Venn diagram:

policy

risk register

continuity plan



>



>



(and repeat!)

Do you have an IT cybersecurity policy or plan?

-----

No

-----

Yes





## TRAINING

Less than half of schools



felt adequately prepared for a cyber-attack or incident



Although social engineering plays a role in many incidents, only



of non-IT staff in schools have received cyber security training











Schools are open to help in this area

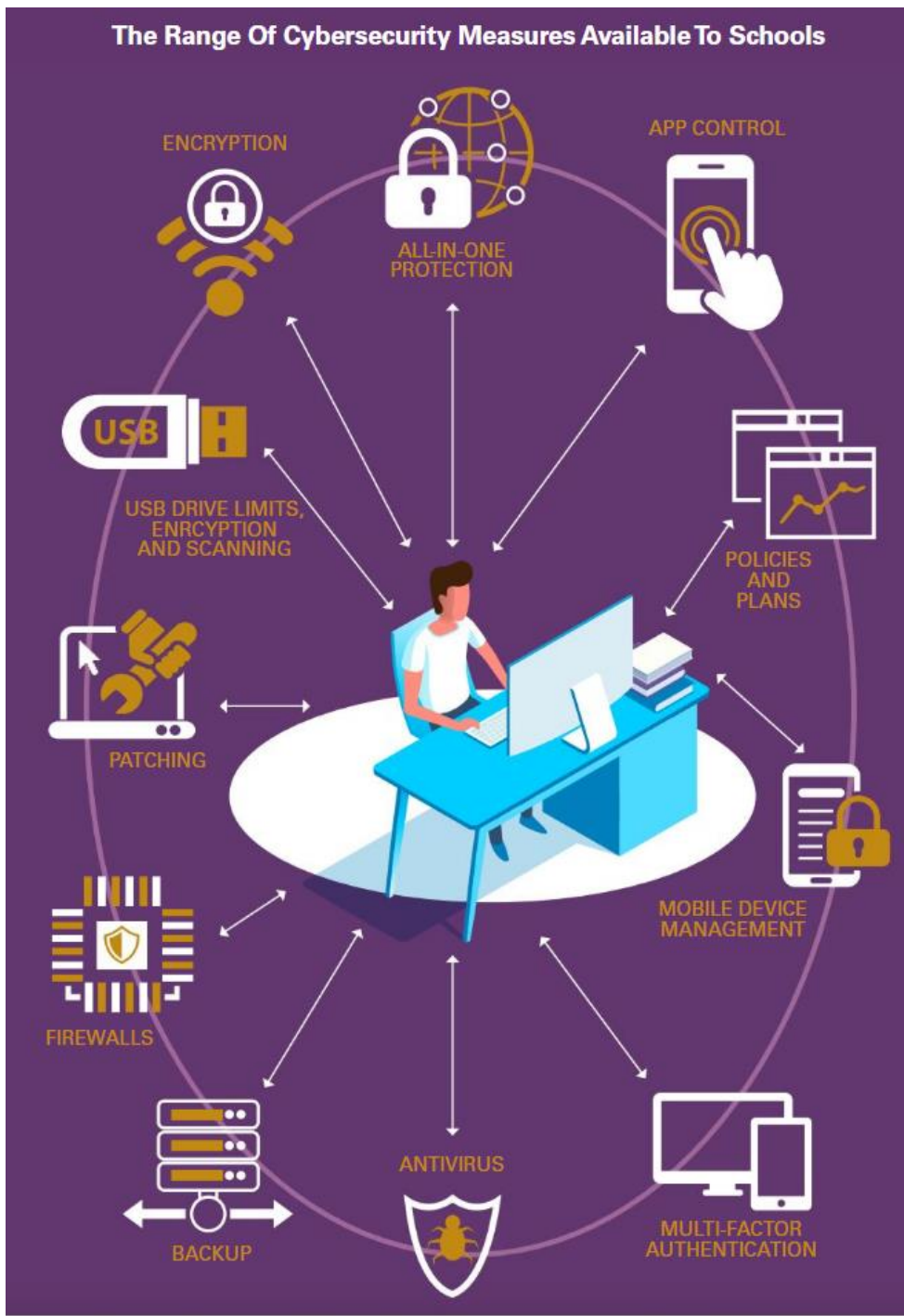


would welcome more cyber security awareness training for staff



## Top Ten Tips For Cybersafe Schools

- 1 Take it seriously** before it takes you seriously 
- 2 Train ALL staff** in cybersecurity – people can be your greatest asset 
- 3 Make sure training** includes policies, systems and general awareness 
- 4 Don't be a circle short of a Venn diagram:**  
policy > risk register > continuity plan  
  
(and repeat!)
- 5 Review** the list of prevention measures we asked about in this survey 
- 6 Follow NCSC password advice** and use MFA 
- 7 Check** that online payment systems are PCI-DSS compliant 
- 8 Ask your broadband and email provider** how they keep you secure 
- 9 Ask all your tech partners** what other services and training they offer 
- 10 Remember** if your school is cybersafe, it will help keep staff and children safe 







**Social:** [@LGfLCyberCloud](#)  
**Newsletter:** [CyberSecurityNews.lgfl.net](#)  
**Videos:** [CyberCloudTV.lgfl.net](#)  
**Research:** [securityaudit.lgfl.net](#)



# DigiSafe

**Social:**

**[@lgfldigisafe](#)**

**Blog:**

**[safeblog.lgfl.net](#)**

**Newsletter:**

**[dslcontacts.lgfl.net](#)**

**Portal:**

**[digisafe.lgfl.net](#)**

**Resources:**

**[saferesources.lgfl.net](#)**

**Videos:**

**[safetv.lgfl.net](#)**