
THE CHALLENGES OF
E-SECURITY
IN SCHOOLS
Network
security

TABLE OF CONTENTS

INTRODUCTION

Today's schools are essentially businesses; they exist to provide learning services and their clients are the students. As in any other business, schools need to ensure the safety and integrity of the data they hold, whilst providing a safe and secure place for students to learn and teachers to teach.

This may sound dramatic, but let's look at what data a school may realistically hold:

- ✓ MIS software which will contain student information, parent/guardian contact details, date of Birth, medical records and other sensitive data.
- ✓ Finance software holds financial and banking information, as well as site asset and personal data.
- ✓ Cashless payment systems containing biometric and possibly financial information
- ✓ Administrative data such as letters to parents, staff contract information, and if you're a larger establishment, any sensitive research information

In this e-book, we'll be exploring some of the challenges that schools face in securing networks and keeping information and users safe.

Journey with us, through the challenges and let us guide you towards what we hope will be enough education, to make informed and educated decisions for your school's network.

Challenge #1: Providing safe and secure working environments

Challenge #1: Providing safe and secure working environments

Security researchers now believe that 2016 will see a marked increase in attacks on schools, because the data they now hold is believed to be 100 times more commercially valuable to hackers. Generally, businesses are now working harder to improve their network security and prevent malicious threats.*

The protection of these systems and their data relies upon security - good security works on a layered approach and it's the combination of these layers that will provide a safe and secure environment.

Security Considerations

The basic and most common level is physical access, for example, you keep your servers in a physically secure environment and control access to the area. Next, you can employ user access permissions via the use of usernames and passwords to control access to the different systems and solutions.

Given the workload on teachers today, many will regularly work from home after school hours, to finish logging the day's events, marking and preparing lessons, so the above protection option is no longer sufficient or efficient for this purpose. This is where Firewalls and Secure Remote Access appliances bridge the gap and play a pivotal role in e-security.

So, what is a Firewall?

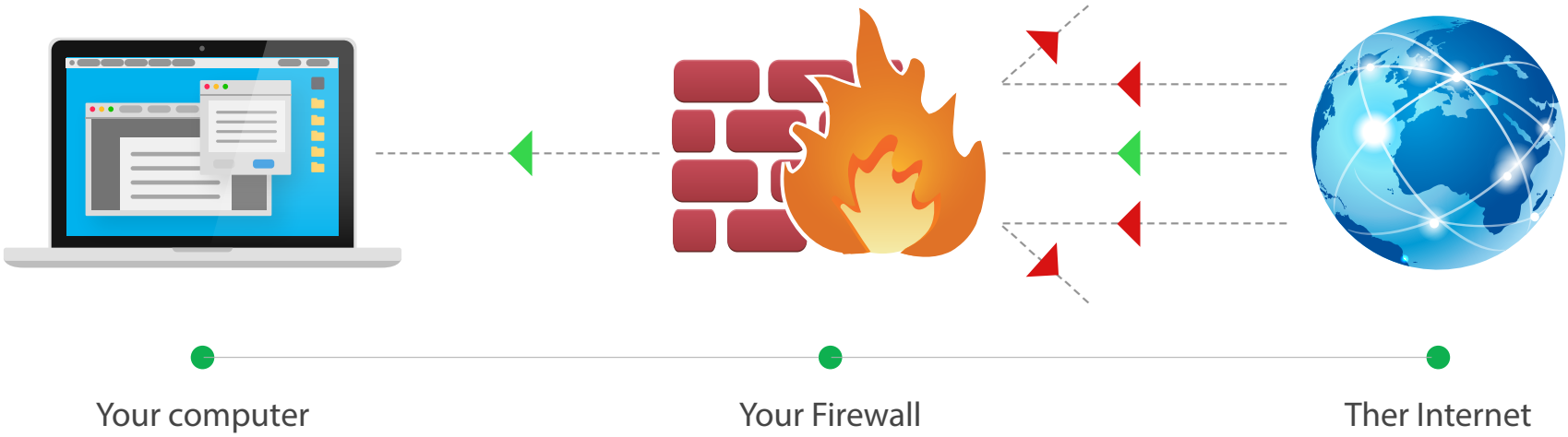
Microsoft's definition of a Firewall is as follows:

'A firewall is software or hardware that checks information coming from the Internet or a network, and then either blocks it or allows it to pass through to your computer, depending on your firewall settings'.*

A firewall can help prevent hackers or malicious software (such as worms) from gaining access to your computer through a network or the Internet. A firewall can also help stop your computer from sending malicious software to other computers as well.

Challenge #1: Providing safe and secure working environments

The following illustration shows how a firewall works.



Just as a brick wall can create a physical barrier, a firewall creates a barrier between the Internet and your computer

'A firewall isn't the same thing as an antivirus program. To help protect your computer, you need a firewall, an antivirus and an anti-malware program.'

This may sound simple, but with all things in the technology arena - hackers, malware and worms - have become more sophisticated, leaving older generation firewalls unable to protect your network from attack or infection.

This is where 'Next-Generation Firewalls' (NGFW) play a part. Next-Generation Firewalls provide multiple network security technologies in one package.

Challenge #1: Providing safe and secure working environments

Are all Firewall's the same?

The answer is simply 'No'.

Modern firewalls are now referred to as Next-Generation Firewalls (NGFW), because they combine the features of traditional firewalls, gateway anti-malware products, intrusion prevention systems and content filtering packages. But more importantly, Next-Generation Firewalls utilize Deep Packet Inspection (DPI) technology to decrypt and inspect SSL (Secure Sockets Layer) traffic into and out of the network, meaning they can detect and block malware concealed in SSL traffic and with more and more organisations using secure web sites by default, it is now a must that you're able to check this traffic.

Next-Generation Firewalls also offer application intelligence and control; they can recognise traffic belonging to specific applications and enforce your acceptable-use policies. They can even allocate bandwidth to high-priority applications.

Challenge #1: Providing safe and secure working environments

Security Considerations

The recent hacks on a number of leading companies just highlights the importance of making sure your security products are up-to-date, correctly configured and more importantly, able to cope with the threats in today's society.

We can summarise the features of a Next-Generation Firewalls as follows:

- ✓ Stop malware, intrusions and advanced attacks
- ✓ Inspect SSL traffic for malicious code
- ✓ Application intelligence and control
- ✓ Visibility into users
- ✓ High performance and scalability

What would we recommend?

This will depend on the client; not all networks are the same and everyone will have different priorities and requirements. This is where consultations with security and network advisors come in. They have the knowledge and understanding to help guide you towards the right product(s) for your network.

That said, as a long-standing Dell SonicWALL partner, we have found that Dell has a good range of security products that will fit most clients and scenarios. Take a look at our case study on page 21 for more information.

It's also worth visiting the Dell SonicWALL website for information – a link can be found in the Useful Links section at the back of this e-book.

Challenge #2:
E-Security Trends & Beyond: Cyber-Security Threats

Challenge #2 – E-Security Trends & Beyond: Cyber-Security Threats

Security threats are constantly evolving. Just as we think we have secured one area, cyber criminals change their attack front or find another loophole to exploit. Whilst this is potentially a nightmare scenario, the secret is not to lose too much sleep over this. And whilst there is a lot of frightening newsprint around cybercrime currently, by ensuring that you have covered the basics it is possible to minimise your risk.

The following are some of the threats we see rising to predominance in **2016** and beyond.

1) Ransomware

Ransomware is the process whereby the criminals infect your machine with a program that first identifies all your data, both local and network, then it encrypts this data using a strong encryption algorithm.
Once encrypted it flashes up warning on screen that you have to pay a ransom to get your data back. This is irrecoverable, once infected you cannot decrypt the data without the correct key. Many people have paid the ransom and to be fair many have had their data unlocked - but many haven't and have ended up losing money and their data.

There is only one protection against Ransomware, backups. Once infected your only recourse is to either pay the ransom and hope, or go to a backup before you were infected. There are plenty of programs that will remove the ransomware but none will decrypt your data, so the secret is to back up everything, at least once a day or even more.

Are your backups working, are you certain?

2) Basic security threats

The single biggest threat to cyber security is home users and workers and the biggest malware and virus threats are attacking security issues that were fixed years ago. It is estimated that there are still millions of computers that are still infected with the Conficker worm even though the security holes and Anti-Virus (AV) programs have been able to clear this problem for years.

You must train your staff and students that it is vital to patch and update their computers at home at least once a month and of course this goes for your establishment systems as well. Also the old chestnut about Mac and Linux machines not being infected is a myth

Oh by the way, did we mention backups…?

3) Social Engineering & Phishing

This is probably the largest frontline in the war on cybercrime. Believe it or not there are simply not thousands of hackers out there spending hours trying to find evermore cunning ways to hack into your network; it is much easier and quicker for them to get your staff to do it for them.

Challenge #2 – E-Security Trends & Beyond: Cyber-Security Threats

A recent survey by 'PhishMe' found that 49% of education users responded to a test phishing e-mail.

Training is the key in this area; the same survey by PhishMe found that after only ten minutes of training, they could reduce the levels of phishing respondents by **97%.** Train your students and staff on how to recognise social engineering and phishing e-mails.

4) Malvertising

Cyber criminals are now investing to further their aims. We have all seen the advent of HTTPS web sites such as Google and Facebook, a move that was designed to make these sites more secure. Unfortunately it has had exactly the opposite effect, the cyber criminals are now paying to place advertisements onto completely legitimate sites, and these adverts carry a malicious payload which, because the site is HTTPS encrypted, bypasses all of your perimeter security such as firewalls and anti-virus.

The previous chapter focused heavily on the need to have reliable firewall protection in place and our prediction serves as a reminder of how necessary this protection really is.

5) Mobile Malware

There have been predictions about the growth of this threat for at least the last two years; however we are predicting that with the rise of BYOD and users actively wanting to use their own devices, criminals will more and more see these as a method of attacking your network.

Smartphones today have greater processing power than was used aboard the space shuttle. As an example of the lengths the criminals will go to, at the end of last year we heard about XcodeGhost, a malware version of Apple's iOS development tool. Again, completely innocent developers used this to develop and publish their apps which were able to bypass Apple's stringent procedures for publication through the App Store. At the time that it was announced it was estimated that 500 million devices were affected.

In the next chapter, we'll be concentrating on BYOD and we'll cover this area in more depth.

6) Data Protection

So what's even better than a healthcare record? Apparently, student records! We are learning that the amount of data collected about our kids over their lifetime as a student is staggering and it even includes some of their health records to boot, which is already one of the richest PII datasets. This, combined with the more open network environment found in educational facilities is why experts anticipate school-based cyber-crime to increase significantly.

Challenge #3:
Bring Your Own Device (BYOD)

Challenge #3: Bring Your Own Device (BYOD)

Bring Your Own 'Disaster'?

Bring your own device (BYOD) is the term used to describe the connection of a personally-owned device (such as a laptop, smartphone or tablet) to a Wi-Fi network provided by a company or other organisation such as a public library, university or school.

The increasing personal ownership of smartphones, tablets and other Wi-Fi enabled devices means more and more public spaces are seeking to make Wi-Fi connectivity available. Sometimes the rationale for doing so is primarily commercial. For example, in restaurants and cafés, free Wi-Fi access can drive increased footfall and revenues as a result. In other instance, the main driver is the public interest, for example in libraries and museums, where providing Internet access to the public is now a priority. Many companies now recognise the importance and opportunity of BYOD to increase productivity and raise employee satisfaction, allowing staff to connect their own devices to corporate networks in a safe, secure way.

There is currently a move away from prohibiting the use of personal devices in managed network environments. However, the successful implementation of BYOD is dependent upon policies, infrastructure and training to ensure that networks are not compromised, data is kept secure and that users are protected as far as possible.

BYOD In schools

BYOD is a growing trend in educational institutions and according to an Ofsted survey carried out during school inspections, 30 per cent of secondary schools now operate a BYOD policy.

So let's first look at the benefits BYOD offers to schools,

Challenge #3: Bring Your Own Device (BYOD)

along with an introduction to the range of challenges that you should consider when deciding to implement your own BYOD policy:

BYOD benefits for schools

- ✓ BYOD offers the potential for increased access, approaching or meeting 1:1 pupil: device ratios in schools;
- ✓ Provides personalisation opportunities, encourages flexibility & self-directed learning, provides a bridge between formal and informal learning;
- ✓ Device portability makes for easy transfer between home and school, for increased pupil and parental engagement;
- ✓ Productivity and efficiency benefits for staff;
- ✓ Meets learner and staff expectations – libraries, cafés and other public places provide free Wi-Fi access – why shouldn't schools do the same?
- ✓ Newer devices offer additional benefits: the battery life of an iPad or Android tablet is typically sufficient to last a school day without re-charging;

Challenge #3: Bring Your Own Device (BYOD)

- ✓ BYOD provides synergy with the move towards cloud-based services, where online services are hosted outside the school to ensure ease of access from the home and elsewhere.

NB: While it is attractive to consider reduced expenditure on devices as a key benefit of BYOD, it is important to remember that the increased network management costs and overheads involved in implementing BYOD properly are likely to counterbalance or outweigh any savings in this regard. Reducing institutional expenditure on devices should not be the primary driver for considering BYOD.

BYOD issues and risks to consider

There are many clear benefits to incorporating the use of BYOD in your school; however, it is important to take a balanced view on this topic, and despite the many benefits, BYOD also a darker side that should be considered. If not fully understood and regulated, BYOD can threaten a school's security and put sensitive information at risk. As a data controller, it is a school's responsibility to make sure any personal data taken home by staff, or accessed on site using a personal device, is kept safe and secure. So here are the risks that any organisation should consider when implementing a BYOD scheme:

- ✓ Potential security risks from allowing personal, unmanaged devices to connect to a managed network;
- ✓ Safety issues - theft (in or on the way to/from school), breakages and insurance costs need to be considered;
- ✓ Financial considerations – how to support learners without a device?
- ✓ Bring Your Own Distraction – in a classroom setting, the use of personal devices, can prove to be a significant distraction for pupils and can disrupt the learning environment.

Challenge #3: Bring Your Own Device (BYOD)

- Device choice – different types of device have very different capabilities; it is important to consider best value rather than lowest cost;

  Local area network (wireless) and broadband capacity considerations – multiple devices and applications all being used simultaneously are likely to place a significant load on both institutional networks and broadband connections, in terms of both upload and download requirements;

- Power management and re-charging considerations – increased reliance on devices increases the importance of sufficient power provision;

- Financial considerations – how to support learners without a device?

- Bring Your Own Distraction – in a classroom setting, the use of personal devices, can prove to be a significant distraction for pupils and can disrupt the learning environment.

- Devices with 3G/4G capability can bypass school networks and services (such as filtering) altogether if network coverage is available in the school – given these devices also have Wi-Fi capability, providing managed access via a BYOD strategy can mitigate this. Requiring that 3G/4G capabilities are turned off when such devices are used in school is one potential approach but may be difficult to enforce;

- Provisioning costs, network management overheads – total cost of ownership (TCO) considerations

Challenge #3: Bring Your Own Device (BYOD)

Implementing BYOD – policies, procedures and technology options

The first and best defence in securing personal devices is to approach it with the same requirements you apply to devices that are already in the school network.

This should include:

Having clear policies in place

Make sure you have a clearly defined policy for BYOD that outlines the guidelines and states up front what the expectations are. This should lay out minimum security requirements as well as including what is not acceptable and why.

Enforcing strong passcodes on all devices

Such policies should include controlling access to the data or device using a password or PIN, and encrypting the data. You should remember that the loss or theft of the device is not the only means by which unauthorised or unlawful access may occur.

For example, a device may be shared amongst family members in a way that is inappropriate if personal data is stored on it.

Monitoring devices in use

All members of staff should log which personal devices they will be using for work purposes and identify the type of storage media on the device. Some devices may use an easily removable memory card, such as a micro or mini SD card, meaning that a loss or theft of data may go unnoticed for some time. Monitoring what is in use will ensure all devices can be accounted for.

Certainly the perceived data security risks can act as a barrier to deploying BYOD and yet the potential of this trend for schools is enormous. So long as the right processes are in place,
BYOD can lead to countless benefits including improved up-take in the use of new technology, overall morale increase, increased job efficiency and increased flexibility.

Challenge #3: Bring Your Own Device (BYOD)

Here are some policy, technology and procedural options for BYOD schemes.

- ✓ Acceptable usage, terms and conditions – a BYOD strategy will require substantial additions and amendments to existing school IT acceptable use policies (AUPs);
- ✓ Technical support considerations – to what extent can a range of different devices be supported? It is important to define learner/parent/staff responsibilities as clearly as possible;
- ✓ Outline specifications for devices for use in school, setting minimum requirements, can form the basis of helpful purchasing advice for parents and can help to standardize the range of devices;
- ✓ The level of access afforded to personal devices needs to be considered and planned carefully (Internet, network services and resources, device

Challenge #3: Bring Your Own Device (BYOD)

management); staff-owned and learner-owned devices will require different levels of access;

- ✓ Technology approaches need to be evaluated and resourced appropriately e.g. managed wireless, guest access, virtual local area networks (VLANs) and network separation/segregation, network access control (NAC), network access protection (NAP), mobile device management (MDM), IP addressing.
- ✓ Broadband performance and capacity need to be assessed in the light of BYOD strategies; an increase in the number of connected devices can place significant additional demands on school networks and broadband connections;
- ✓ Staff and learner training will be needed, on BYOD policies, procedures and infrastructure requirements.
- ✓ Specialist activities (e.g. graphic design, CAD) will still require specific hardware to run and cannot yet be accommodated via BYOD.

Case Example: Schools falling short on Wi-Fi connectivity

Schools have been urged to ensure that Wi-Fi access is freely available in the classroom following a survey which revealed that half of school IT managers were not satisfied with their Wi-Fi deployment.

Some 92% of the 560 IT decision makers quizzed in the research said that high-quality Wi-Fi is an invaluable resource for teaching and learning, but only 42% feel their Wi-Fi is visible enough to support students.

Although the study, commissioned by Aerohive Networks, is not UK-specific, it suggests schools worldwide are not investing enough funds in Wi-Fi technology to see its full potential.

Challenge #3: Bring Your Own Device (BYOD)

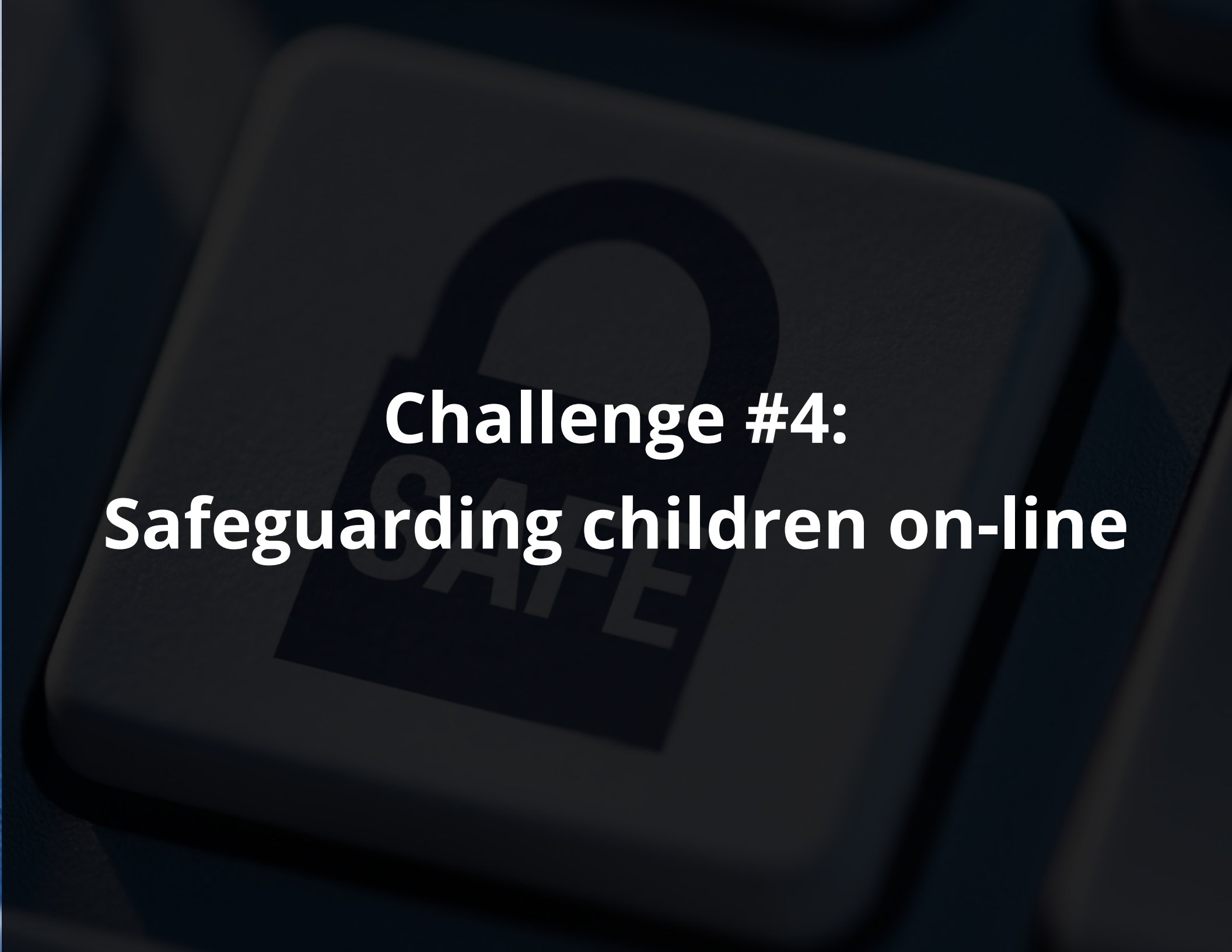
Perhaps that will all change sooner rather than later, with three-quarters of schools actively encouraging BYOD (bring your own device) initiatives, and believing proper Wi-Fi connectivity can improve learning.

However, only 42% of respondents said they were equipped to handle this influx of new devices, while a lack of network intelligence means many cannot meet their school's Wi-Fi demands.

As a result, nearly all respondents (95%) said teachers and students aren't satisfied with school Wi-Fi systems.

"When teaching resources can't be loaded, or programmes stall and crash, this eats into children's learning time. Schools cannot afford to fall behind in digital learning," stressed Paul Hennin, senior director of international marketing at Aerohive Networks.

"This research demonstrates that better connectivity improves the learning experience for students and provides a more personalised approach to teaching. Having uninterrupted access to educational tools and apps provides teachers with the ability to have full visibility and control over students' online activity, and keep them focused at the task at hand."



Challenge #4:
Safeguarding children on-line

Challenge #4 – Safeguarding children on-line

What is safeguarding?

Safeguarding is the action that is taken to promote the welfare of children and protect them from harm. Safeguarding means:

- ✓ Protecting children from abuse and maltreatment
- ✓ Preventing harm to children's health or development
- ✓ Ensuring children grow up with the provision of safe and effective care
- ✓ Taking action to enable all children and young people to have the best outcomes.

Safeguarding children and child protection guidance and legislation applies to all children up to the age of 18.

Online Safety

A March 2015 Ofsted survey revealed that over 25% of secondary students cannot recall if they have been taught about online safety over the last 12 months. 9% of primary staff also believed that they had not had effective training in the 12 months prior to March 2015.

There is acknowledgement that teachers have a responsibility to educate parents, as well as children about the potential dangers that are present online. The Department for Education (DfE) July 2015 statutory guidance "Keeping children safe in education" has clarified government expectations for e-safety in schools. This guidance has since been supported by the new September 2015 Ofsted common inspection framework which evaluates e-safety as a key measurement across all judgement areas.

We must also equip children with the right skill-set to use online resources in a safe, responsible manner.

Challenge #4 – Safeguarding children on-line

It's all about student knowledge, protection the school's networks and the ebb and flow of data.

Monitoring and filtering, rather than blocking, is essential to prevent access to inappropriate content, for example, banning Facebook or social networking sites could actually leave students more vulnerable when they are outside the school gates if they don't get to learn how to use social media safely within a safe, secure environment.

Sex and Relationships

For today's young people, experiences around sex and relationships are hugely influenced by the internet and digital technology, which play such an important role in young people's lives and their emotional development. It is essential that schools ensure that their sex and relationships education is fit for the 21st century, covering issues such as pornography, sexting and healthy digital relationships.

Challenge #4 – Safeguarding children on-line

Explicit content

A 2014 academic report found that 17% of UK children aged 9-16 have seen sexual images online or offline in the last year, with over half saying they had been upset by these images.

Sexual or pornographic content is easy to find – online, in advertising, music videos and wider – and it is incredibly important that we facilitate discussions with children about the issues surrounding exposure to this kind of content.

Pornography can depict a lack of communication about choices, sexual consent and contraception, and often shows violent and oppressive behaviours towards women, which can be frightening and confusing, make young people feel pressured to behave in particular ways.

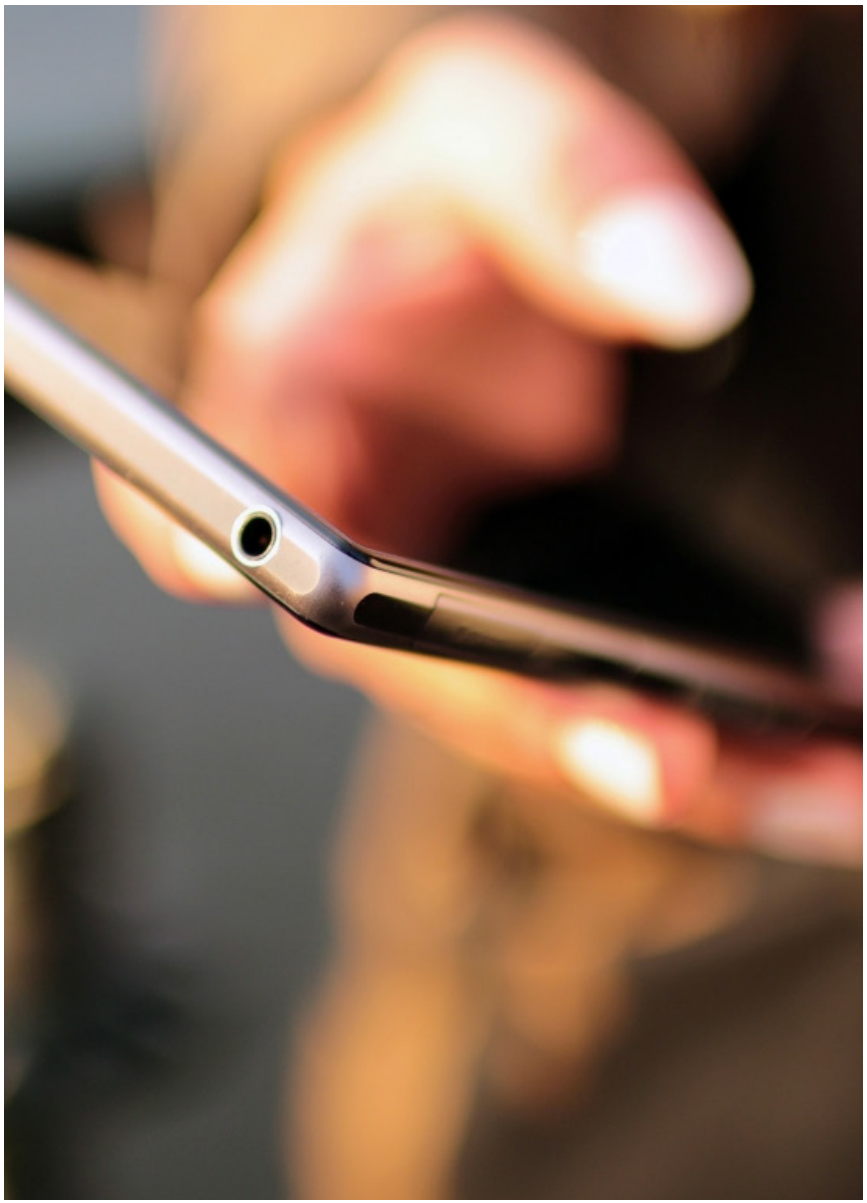
It is important that schools provide an alternative narrative to the content children are being exposed to online, and help young people critically assess pornographic content and safeguard themselves.

Inappropriate Imagery/Messaging

Sexting is the sending of sexually explicit images. Students need to be made aware of the law and how it is illegal to produce, possess or distribute an indecent image of a person under 18. With a reported 60% of teenagers being asked online for a sexual images or videos of themselves, it is clearly an issue we need to be helping young people with. Furthermore, young people need to recognise grooming behaviours and know when and how to report incidents.

A 2014 report found that 1 in 20 UK children aged

Challenge #4 – Safeguarding children on-line



11-16 years have received a sexual message online, and 17% of UK children aged 9-16 have chatted to strangers online.

Healthy Relationships

Young people can feel pressured by partners to communicate frequently or share passwords; and jealousies and control can be a real problem online.

Personal, Social, Health and Economic education

Cyberbullying, healthy digital behaviours, privacy, online reputations, and safe social networking are also key topics that surround the safe and positive use of technology.

It is important that issues such as these are addressed within schools and that teacher's feel trained and

Challenge #4 – Safeguarding children on-line

equipped to effectively address a wide range of issues. E-safety is a subject that needs to be addressed and reinforced across all subjects in the curriculum, in particular in PSHE and SRE, where more sensitive issues can be discussed in more depth.

Taking Control

E-Security isn't only about firewalls and web page monitoring, although these things help significantly, it is essential that we ensure that young people are equipped to protect themselves from harm online, for times when they are not in the school environment. Research shows the range of risks that young people are exposed to online:

- ✓ *12% of 9-16s have been cyberbullied, with 21% saying they had been treated in hurtful or nasty way online.*
- ✓ *17% of 11-16s have seen websites where people discuss ways of physically harming or hurting themselves, with 1 in 25 having seen suicide websites.*
- ✓ *14% of 11-16s have seen sites that promote eating disorders; rising to over 1 in 5 young people aged 13-14 years.*

Whilst safety measures can be taken to ensure secure networks and visibility of activity whilst in school, education is the most important factor when it comes to keeping children and young people safe on the internet – technical tools are important, but education gives them knowledge and responsibility for their own well-being.

PREVENT

But, it's not just cyber-bullying and inappropriate content that is an issue for future generations. From 1 July 2015, all schools and childcare providers must have due regard to the need to prevent people being drawn into terrorism.

Challenge #4 – Safeguarding children on-line

What is the Prevent duty?

The government has defined extremism in the Prevent strategy as: "vocal or active opposition to fundamental British Values, including democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths and beliefs."

Childcare and Early Years Providers subject to the Prevent duty will be expected to demonstrate activity in the following areas:

- ✓ Assessing the risk of children being drawn into terrorism.
- ✓ Demonstrate that they are protecting children and young people from being drawn into terrorism by having robust safeguarding policies.
- ✓ Ensure that their safeguarding arrangements take into account the policies and procedures of the Local Safeguarding Children Board.

- ✓ Make sure that staff have training that gives them the knowledge and confidence to identify children at risk of being drawn into terrorism, and to challenge extremist ideas which can be used to legitimise terrorism.
- ✓ Expected to ensure children are safe from terrorist and extremist material when accessing the internet.

Challenge #4 – Safeguarding children on-line

You're probably well versed in the intricacies of Prevent Duty, but just in case, the DfE have produced detailed guidance for schools and childcare providers and we recommend visiting the Gov.uk website for more information (you can find a link to the gov.uk website in the Useful Links section).

There are also monitoring tools that have a catalogue of pre-defined words/phrases which checks against targeted words or phrases in documents and internet searching, along with technology that can be installed on school computers, to pick up phrases popular with jihadist sympathisers such as 'YODO', which means 'You Only Die Once. It was anticipated that up to 40 per cent of secondary head teachers were expected to adopt the software, which is an upgrade of existing anti-bullying technology already used in their schools, however, we now believe this figure will be much higher.

Student Safeguarding Options

It's not just staff that need to get involved – so do students; here are few suggestions that could help you educate students about staying e-safe.

Questions to ask:

What is e-safety?

Start by finding out what students think e-safety is, as a way of gauging their current knowledge.

Responsible social networking

Share a fictitious social network profile and ask students how this person is protecting his/her personal information and what he/she's doing wrong.

Are you a cyberbully?

Was that 'joke' they sent really funny, or could it have been an act of unintentional bullying?

Challenge #4 – Safeguarding children on-line

What's your digital footprint?

What information is there about them online and how best to protect online reputations (now and in the future); what do they know about sharing personal information.

Fact or fiction

How to investigate what they might think are 'facts' found online


Challenge #5:
Moving forwards

Challenge #5 – Moving forwards

The whole subject of e-security can be quite overwhelming, so we hope that we've imparted useful and honest information in a simple and uncomplicated way.

As a quick precursor, we're listing what we feel are the most important points we've raised during this series:

- ✓ Invest in a good firewall
- ✓ Lock down your data flow by using Secure Remote Access
- ✓ Get your network backed-up!
- ✓ Train staff and students about malware and social engineering emails
- ✓ Implement BYOD policies, procedures and technology options
- ✓ Include both staff and students in educating and training on safeguarding measures

Challenge 1: Providing safe and secure working environments

To recap: We already know that today's schools are essentially businesses; providing learning services to students. As in any other business, schools need to ensure the safety and integrity of the data they hold, whilst providing a safe and secure place for students to learn and teachers to teach.

The protection of these systems and their data relies upon security - good security works on a layered approach and it's the combination of these layers that will provide a safe and secure environment.

Consider network security, firewall protection and SRA requirements as the building blocks required to keep the school's IT infrastructure safe and secure. It's that simple.

Challenge #5 – Moving forwards

Already thinking about your summer holidays? Will your network be resting or ready?

Here's our quick checklist to make sure everything will be tip-top:

- ✓ Is your wireless network safe from intrusion and inappropriate usage?
- ✓ Are you getting the best performance from your available internet speed?
- ✓ Are you checking that children aren't using non-school issued devices on the school network to bully or browse unsafe websites?
- ✓ Are your school-issued devices protected from viruses, Trojans, spyware and the latest 'watering hole' attacks?
- ✓ Have you ensured your staff aren't impeded by tedious and cumbersome IT security procedures?

If the answer to any of the above is no, call us on **0208 660 1730** and find out how we can give you complete internet and network security peace of mind!

CHALLENGE 2 - Security Threats

To recap: Security threats are constantly evolving. Just as we think we have secured one area, cyber criminals change their attack front or find another loophole to exploit. Whilst this is potentially a nightmare scenario, the secret is not to lose too much sleep over this. And whilst there is a lot of frightening newsprint around cybercrime, by ensuring that you have covered the basics it is possible to minimise your risk. We listed the threats that we consider to be the most relevant for this year and below we offer some viable solutions

Ransomware and other more basic security threats

There is only one protection against Ransomware, backups. Once infected your only recourse is to either pay the ransom and hope, or go to a backup before you

Challenge #5 – Moving forwards

were infected. There are plenty of programs that will remove the ransomware but none will decrypt your data, so the secret is to back-up at least once a day or even more.

Are your backups working, are you certain?

Basic security threats

You must train your staff and students that it is vital to patch and update their computers at home at least once a month and of course this goes for your establishment systems as well. Also the old chestnut about Mac and Linux machines not being infected is a myth - if you still believe this then you are part of the problem.

Oh by the way, did we mention backups…?

Social Engineering & Phishing

Training is the key in this area; the same survey by PhishMe found that after only ten minutes of training, they could reduce the levels of phishing respondents by 97%

Train your students and staff on how to recognise social engineering and phishing e-mails.

Malvertising

Firewall protection is the best and most efficient way to protect yourself. Our prediction serves as a reminder of how necessary this protection really is.

There are also additional measures you can take to protect your working environment, including:

- ✓ Adopting user education and acceptable-use policies
- ✓ Enacting password policies
- ✓ Keeping current with updates and patches
- ✓ Utilizing intrusion prevention and gateway anti-malware
- ✓ Deploying application control and content filtering

Challenge #5 – Moving forwards

TOP TIP

The most efficient way to safeguard against a large percentage of outside threats is backups. Whilst you can't completely eradicate the risk of security breaches, worms, hacking, or any of the other threats that exist currently, backing up your data will allow you to get back up and running as quickly as possible, with minimal impact to your staff and students.

Call us if you'd like support or advice on backing up your data.

Challenge 3: Bring Your Own Device (BYOD)

Bring Your Own 'Disaster'?

To recap: Bring your own device (BYOD) is the term used to describe the connection of a personally-owned device (such as a laptop, smartphone or tablet) to a wi-fi network provided by a company or other organisation such as a public library, university or school.

The successful implementation of BYOD is dependent upon policies, infrastructure and training to ensure that networks are not compromised, data is kept secure and that users are protected as far as possible.

Implementing BYOD

We recommend to our clients, the implementation of the following:

- ✓ Have clear policies in place
- ✓ Enforce strong passcodes on all devices
- ✓ Monitor all devices in use

We often write guidelines for schools who need additional support, we provide password advice and guidance on monitoring the external devices that are using your school's network. As with everything, the first and best defence in

securing personal devices is to approach it with the same requirements you apply to devices that are already being used in your school. So long as the right processes are in place, BYOD can be an asset to both staff and students.

If you need any advice or guidance on implementing BYOD effectively, or whether your current policies are sufficient,
call us on: **0208 660 1730.**

CHALLENGE 4 – Safeguarding Children Online

To recap: Safeguarding can be anything from preventing the improper use of websites within the school, through to the direct protection of children from harm whilst outside school.

Taking Control

E-Security isn't only about firewalls and web page monitoring, although these things help significantly. We have experience of independently investigating areas of misuse and inappropriate use of school equipment and as a result, we pride ourselves in our confidential and sensitive approach to such serious matters.

Training, Training and more Training…

Whilst safety measures can be taken to ensure secure networks and visibility of activity whilst in school, we still believe that education is the most important factor when it comes to keeping children, young adults and staff safe on the internet – technical tools are important, but education gives them knowledge and responsibility for their own well-being.

Case Study : Aspire

Case Study : Aspire

"Our staff and students were protected from day one. We don't worry about security breaches or about our students being able to access anything inappropriate. Dell SonicWALL has given us peace of mind."

Greg Hodgson, Deputy Head, Aspire Chiltern Skills & Enterprise Centre

Aspire provides alternative full- or part-time educational provision and support for secondary-age students. One of five centres, Aspire Chiltern Skills & Enterprise Centre (CSEC) is a purpose-built pupil referral unit (PRU) offering full-time provision for students who have been permanently excluded from their mainstream school, as well as part-time provision for students at risk of exclusion. CSEC turned to its trusted IT partner IA Computing and to Dell when needing to swiftly install a firewall to protect its students and staff, as well as its network.

Internet connectivity is vital for learning

Just before CSEC was due to openin 2013, it came to light that the local authority had overlooked the provision of internet connectivity for the PRU. The internet is an important teaching and learning aid for all schools, and PRUs are no exception. Deputy Head Greg Hodgson explains, "At CSEC, we deal with the most vulnerable children who have not previously found school to bea particularly positive experience. Our objective is to get our students working and to teach them boundaries. Using the internet is a huge part of that, both in terms of what we teach and how we teach."

Next-generation firewall needed to protect students, staff and network

Until the local authority was able to rectify the situation

Case Study : Aspire

with its authorised internet connectivity provider, CSEC had no choice but to use its standard phone lines. A firewall was therefore urgently needed, not only to protect the school's network from security breaches, but also to ensure safe internet access for staff and students, and to provide content filtering. IA Computing had been selected to implement CSEC's IT infrastructure and it recommended a Dell SonicWALL NSA 3600 next-generation firewall.

IA Computing offers a range of cost- effective IT services throughout the south east of England, as well as worldwide IT support. One of its main areas of expertise is providing IT for schools, having built up significant experience in addressing the challenges faced by educational establishments.

The Dell SonicWALL NSA 3600 next- generation firewall was suggested to CSEC to deliver enterprise-class security and performance for their mid-sized network.

The appliances would offer the centre integrated, automated and dynamic security capabilities in a single platform, combining the patented SonicWALL Reassembly Free Deep Packet Inspection (RFDPI) firewall engine with a powerful, scalable, multi-core architecture. This would enable CSECto block the most sophisticated threats with an intrusion prevention system (IPS) that features advanced anti- evasion capabilities, SSL decryption and inspection, and network-based malware protection. The latter leverages the power of a continually updated cloud database, to provide protection against the most recent threats.

"Our ethos is to offer our vulnerable students the very best of everything that we can. This includes the protection delivered by our firewall. Dell SonicWALL is the best solution on the market, so we wouldn't want to give it up."

Greg Hodgson, Deputy Head, Aspire Chiltern Skills & Enterprise Centre

Case Study : Aspire

Personalised and conscientious approach instilled trust

CSEC has to be flexible in the way that it approaches teaching its students; many different options are often needed in just one lesson. IA Computing implemented CSEC's much needed multi-platform IT environment, with with PCs and Apple Macs and iPads. "We had chosen IA Computing as our IT partner because we really liked their personalised and conscientious approach to truly understanding our requirements. Therefore, we were more than happy to place our trust in their Dell SonicWALL firewall recommendation," comments Hodgson. Dell SonicWALL was duly implemented, both swiftly and straightforwardly, by IA Computing.

Safe and flexible internet access is delivered to staff and students

Most importantly, CSEC now feels protected and is assured of safe internet access with its new firewall. "Our staff and students were protected from day one," says Hodgson. "We don't worry about security breaches or about our students being able to access anything inappropriate. Dell SonicWALL has given us peace of mind."

SonicWALL's content filtering provides not only barriers, but also the versatility that CSEC needs. "If necessary, we can quickly and easily switch off sites such as YouTube or Facebook, just for an afternoon," says Hodgson. "SonicWALL's flexibility to respond to our day-to-day requirements is invaluable."

Offering the best of everything

The local authority's authorised internet connectivity has since been installed. However, CSEC has insisted on maintaining its next-generation firewall in order to be assured of the protection and flexible content filtering offered by Dell SonicWALL. "We are a growing

organisation, and our ethos is to offer our vulnerable students the very best of everything that we can. This includes the protection delivered by our firewall," comments Hodgson. "Dell SonicWALL is the best solution on the market, so we wouldn't want to give it up."

Minimal firewall admin frees up IT staff

CSEC's use of its new firewall has barely impacted on its IT staff. "Because Dell SonicWALL requires very little ongoing administration effort, CSEC's IT team can focus on delivering other value-added tools instead," notes Hodgson.

Full ROI is delivered

In terms of ROI, CSEC feels that Dell SonicWALL offers true value for money. "Dell SonicWALL is not the cheapest firewall on the market," adds Hodgson. " But the value that it has delivered to us in terms of protection and its low impact on the IT team means that it has most definitely paid for itself."

Aspire has now deployed Dell SonicWALL next-generation firewalls at three further sites, and plans to roll-out more.

About Dell Security

Dell Security solutions help you create and maintain a strong security foundation with interconnected solutions that span the enterprise. From endpoints and users to networks, data and identity, Dell Security solutions mitigate risk and reduce complexity so you can drive your business forward. www.dell.com/security.

"Dell SonicWALL is not the cheapest firewall on the market. But, the value that it has delivered to us in terms of protection and its low impact on the IT team means that it has most definitely paid for itself."

Greg Hodgson, Deputy Head, Aspire Chiltern Skills & Enterprise Centre

Appendix 1 : About Us

Appendix 1 : About Us

Supportive, Honest, Innovative

Founded in 2000 by focused IT professionals, who believed there was a need to bring a fresh approach to the IT culture, IA Computing has developed a wide ranging skillset, with a solid background in partnering with schools.

The founding directors have over 50 years knowledge and experience within the IT industry and combining our principles of being supportive, honest and innovative, together with the experience of our technical staff, allows us to provide a highly professional and affordable service, with a friendly face.

Supportive

Consider us your IT guru, or better still, an extension of your own team. There when you need us, to offer guidance and support, especially on those occasions when it all seems to be going wrong!
We love our tech; we're passionate about problem solving and even better, we get things to work where others have failed.

Honest

We are experts in security solutions and can help you gauge the risks and choose appropriate levels of protection.

Should you need help in defining your IT strategy, choosing technologies, procurement, project management, network security, network infrastructure and installation, speak to us first.

We'll always make it our business to bring cost-effective and efficient IT systems into your business and this can be achieved through our ethos of honest consultancy services.

Appendix 1 : About Us

Innovative

"Think outside the box"… "Stepping up to the plate"… "If you can't stand the heat, get out of the kitchen"

We've all heard the clichés, but in our world, the 'box' doesn't exist, we're building a neat little dinner service and we simply love the kitchen! In all seriousness, whatever it takes, we find a solution, even if it means taking an approach that is slightly out of the ordinary.

Helpdesk

Our Helpdesk is run by a team of professional, friendly and supportive people who will provide you with instant technical support as and when you need it.

We will actively encourage you to use the service desk to ask any 'How Can I?' questions - these can be from the very easy to the real head-scratchers. Our comprehensive call logging system does the boring admin jobs for you; it can record and track your support history, keep an inventory of the equipment you have purchased, and set reminders for licence renewals; our helpdesk team are nothing short of happiness itself when taking your calls and even better, calls to us are standard rate – we don't believe in charging you premium rates to receive support from us.

To read more about how we can help you – go to:

http://www.iacomputing.co.uk/

http://www.iacomputing.co.uk/it-services-surrey/it-services-for-education

http://www.iacomputing.co.uk/it-services-surrey/it-services-for-education/managed-it-services

http://www.iacomputing.co.uk/it-services-surrey/it-purchasing-service

http://www.iacomputing.co.uk/honest-advice/good-it-support-company

References & Resources

References & Resources

E-Security Trends & Beyond: Cyber-Security Threats

Trends: 'Security Predictions of 2016' from Wickhill

http://www.wickhill.com/uploads/vendors/Watchguard/watchguard_2016_security_predictions_ebook.pdf

https://www.youtube.com/watch?v=uqJBKMurYzk

The BETT Show

http://www.bettshow.com/library/Does-allowing-children-to-bring-their-mobiles-into-school-have-the-potential-to-offer-educational-advantages-1-2-3

BBC micro:bit (https://www.microbit.co.uk/#)

HP Sprout (http://www8.hp.com/uk/en/sprout/home.html)

BYOD

E-learning Foundation -

http://www.e-learningfoundation.com/

Misco IT News - Feb -

http://www.misco.co.uk/blog/news/03720/schools-falling-short-on-wifi-connectivity

CDW-G: Bring Your Own Device: Preparing for the influx of mobile computing devices in schools

CDW-G: Bring Your Own Device: Adapting to the flood of personal mobile computing devices accessing campus networks

Cisco: BYOD in education

Cisco: BYOD Security Challenges in Education: Protect the Network, Information, and Students

http://www.e-learningfoundation.com

Microsoft: Bring your own device to school

Meru Networks/Samsung: One-to-One 2.0: Building on the "Bring Your Own Device" (BYOD) Revolution

http://www.nen.gov.uk/

RM: Bring your own device

References & Resources

Safeguarding

PREVENT Guidance and Information

https://www.gov.uk/government/publications/prevent-duty-guidance

https://www.gov.uk/government/publications/protecting-children-from-radicalisation-the-preventduty

The use of social media for online radicalisation: Guide for schools on how terrorist groups such as ISIL use social media to encourage travel to Syria and Iraq:

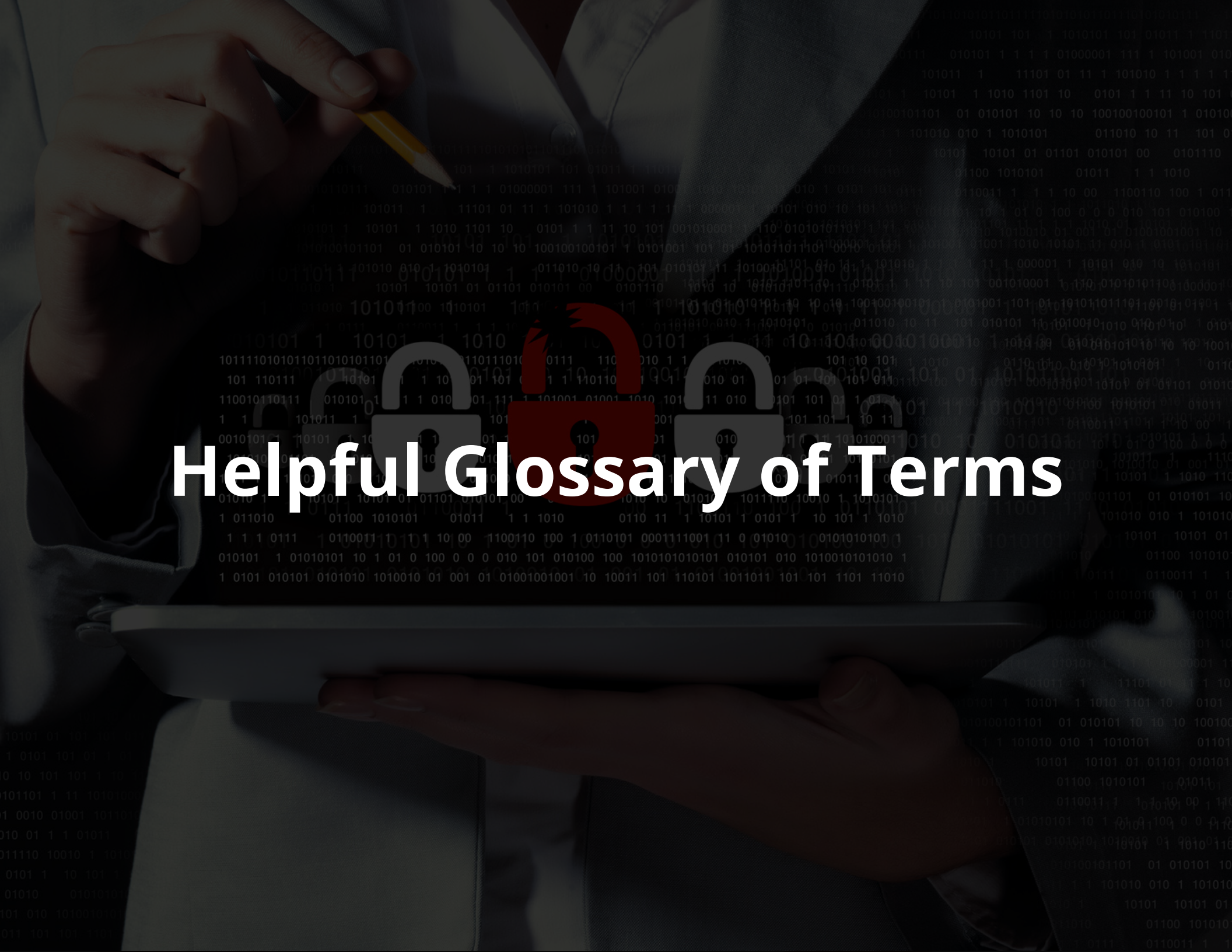
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/440450/How_social_media_is_used_to_encourage_travel_to_Syria_and_Iraq.pdf

Keeping children safe in education Information for all school and college staff:
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/447596/KCSIE_Part_1_July_2015.pdf

https://www.nspcc.org.uk/preventing-abuse/safeguarding/

Child Exploitation and Online Protection Centre - Understanding Online Social Network Services and Risks to Youth.

Mascheroni & Ólafsson (2014) Net Children Go Mobile: risks and opportunities



Helpful Glossary of Terms

Helpful Glossary of Terms

Anti-spam software - the method that detects e-mail messages that are unsolicited advertisements, called "spam." A spam filter is used to detect spam and divert it to a spam folder (junk mailbox).

Anti-Virus (AV) - Antivirus (or anti-virus) software is used to safeguard a computer from malware, including viruses, computer worms, and Trojan horses. Antivirus software may also remove or prevent spyware and adware, along with other forms of malicious programs.

Botnets - A bot is a small piece of malicious software. And a botnet is a network of computers that have been infected with it, without the owners' knowledge or permission. Controlled as a group, botnets are often used to send spam, support denial-of-service (DDoS) attacks against websites, engage in cybercrime, act as electronic spies, steal people's identities and even remove money from bank accounts.

BYOD – Bring Your Own Device

Conficker - also known as Downup, Downadup and Kido, is a computer targeting the Microsoft Windows operating system that was first detected in November 2008.

Cookies - Cookies are small text files added to your computer when you visit websites. They are usually completely harmless, just containing a website name and unique user ID.

Cyberbullying - Cyberbullying is simply bullying carried out online. Just like in real life, children and teens are most likely to engage in cyberbullying and they're also the most likely to be bullied online themselves.

Domain Name - Domain names are mainly used in web addresses such as somewhere.co.uk and in email addresses - firstname.lastname@somewhere.co.uk.

A domain name is a string of letters and numbers used to name organisations, computers and addresses on the internet.

Helpful Glossary of Terms

Domain name registrar - A registrar is the company or organisation that people register their domain name through. This may be an ISP or a domain name reseller or just a company that specialises in registering domain names.

Dongle - A mobile dongle is a piece of technology, usually the same size as a USB/flash memory stick that plugs into a computer, laptop or netbook and provides mobile access to the internet through the use of traditional mobile phone networks. Mobile broadband dongles are available to purchase on most major phone networks and can be on a monthly contract or pay as you go tariff.

Firewall - A firewall protects your machine, whether it's part of a work network or a home PC, against the outside world. It helps prevent incoming malicious software like viruses, spyware, hackers, Trojans and other malware getting inside your machine and causing damage. It's very like a real-life, physical firewall which prevents fire from spreading from one area to another.

Flickr - Flickr is an easy way to upload and share your photos to the web.

Malvertising (a combo of "malicious advertising") is the use of online advertising to spread malware. Malvertising involves injecting malicious or malware-laden advertisements into legitimate online advertising networks and webpages.

Malware – Malware is an umbrella term used to refer to a variety of forms of hostile or intrusive software, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, scareware, and other malicious programs. It can take the form of executable code, scripts, active content, and other software.

Helpful Glossary of Terms

MiFi - A portable device that transmits a Wi-Fi signal using a mobile network in much the same way as a mobile phone connected to the internet. Multiple Wi-Fi capable devices can connect to one MiFi transmitter and share the mobile internet coverage. The word MiFi is the merge of Mobile and Wi-Fi.

Mobile device management (MDM) - Is an industry term for the administration of mobile devices, such as smartphones, tablet computers, laptops and desktop computers. MDM is usually implemented with the use of a third party product that has management features for particular vendors of mobile devices.

Network Access Control (NAC) - is an approach to computer security that attempts to unify endpoint security technology (such as antivirus, host intrusion prevention, and vulnerability assessment), user or system authentication and network security enforcement.

Network Access Protection (NAP) - is a Microsoft technology for controlling network access of a computer, based on its health. With NAP, system administrators of an organisation can define policies for system health requirements.

PhishMe - Phishing can be defined as any type of email-based social engineering attack, and is the favoured method used by cyber criminals to carry out malware and drive-by attacks. These are fraudulent emails disguised as legitimate communication that attempt to trick the recipient into responding – by clicking a link, opening an attachment, or directly providing sensitive information.

Ransomware – Ransomware is a type of malware that prevents or limits users from accessing their system. This type of malware forces its victims to pay the ransom through certain online payment methods in order to

Helpful Glossary of Terms

grant access to their systems, or to get their data back. Some ransomware encrypts files (called Cryptolocker).

Sexting is when someone sends or receives a sexually explicit text, image or video on their mobile phone, usually in a text message

Scareware - Scareware is a type of malware. It's designed to trick people into buying and downloading potentially dangerous software. Scareware usually comes in the form of pop-ups. They often look exactly like operating system messages, for example Windows messages, and commonly pretend to be from antivirus, antispyware, firewalls and registry cleaners, announcing they've discovered problems with your system and asking you to click to buy and run software to fix things. In reality, the problems are fictional.

Snapchat - Snapchat is a time-limited phone photo-sharing app for iPhone, iPad and Android smartphones, which allows users to send images to each other that 'self-destruct' within one to ten seconds of being viewed. Users can send video clips in addition to images, which are deleted from the servers after they have disappeared.

Social engineering - This is where an outside hacker makes use of psychological tricks on legitimate computer system users in order to obtain information (such as a password) to gain access rather than breaking into the system.

Spam - is usually considered to be electronic junk mail or junk newsgroup postings. Some people define even more generally as any unsolicited email.

Helpful Glossary of Terms

Trojans - Trojan horse is a program that claims to rid your computer of viruses but instead introduces viruses onto your computer.

Trolling - Purposely spreading hatred, racism, misogyny, bigotry, conflict and any other kind of unpleasantness. It's often political, social or cultural. But when a troll posts abusive and hurtful comments about a specific person, it's called flaming. Either way, it's anonymous.

Twitter Spam - The act of following mass numbers of people, not because you're actually interested in their tweets, but simply to gain attention, get views of your profile (and possibly clicks on URLs therein), or (ideally) to get followed back.

Virtual Private Network (VPN) - A Virtual Private Network (VPN) is a private network that uses a public network such as the internet to securely connect remote sites or users together. Instead of using a dedicated, real-world connection such as leased line, a VPN uses 'virtual' connections via the Internet from the company's private network to the remote site or employee.

WAN – Wide-Area Network

WiBro – Wireless Broadband

Wi-Fi – Wireless Fidelity

Worms - These viruses are designed to cripple computer systems and networks. Once they're out there, they don't need to be sent – they'll scan the internet themselves to find computers running specific programs that they can infect.

IA Computing Ltd
1 Redlands Business Centre
Redlands
Coulsdon
Surrey
CR5 2HT

Tel: 020 8660 1730

Email: esecurity@iacomputing.com

www.iacomputing.co.uk