geekapedia

Top 10 tips to help you release your inner geek

SOPHOS

Security made simple.

geekapedia

No stress. No hassles
We'll show you how

Think about it. Ofsted inspectors want to know you're protecting students and staff in the use of technology, and what measures you have in place to intervene if a problem occurs.

It doesn't have to be difficult. To inspire you we've put together this geekapedia. Use these technical and common-sense reminders for staff and students and you'll have a stress-free Ofsted inspection, and more time to relax and release your inner geek.

CLASS NETWORKS

SOPHOS
Security made simple.

geekapedia

Contents

CLASS NETWORKS

SOPHOS
Security made simple.

1. Your e-safety policy

Take the time to review your e-safety policy now and make sure it's everything it should be. It's the best way to make sure your next Ofsted review is a breeze.

Essentially, your policy should outline:

- Your ability to protect and educate pupils and staff on the use of technology
- Systems in place to intervene and support if any incident arises

As technology changes, so do Ofsted's guidelines for e-safety. The impact of technology is the focus, with the need for institutions to take a consistent and effective approach. So what does Ofsted consider effective practice for outstanding schools and colleges?

Essentially, it falls into four themes:

Make it part of the curriculum

Students need to understand acceptable online behaviour, and how to act in a safe and appropriate way. Digital literacy is key.

CONSIDER: Don't leave e-safety issues to the occasional lesson. Embed it into the entire curriculum.

Whole-school/college approach

Students, teachers, and non-teachers should recognise e-safety issues. This should be a priority and include a commitment to training, developing policies, and a straightforward, consistent approach when addressing an incident.

CONSIDER: If you don't already have one, appoint an e-safety co-ordinator to provide a consistent point of contact on these issues. This doesn't have to be you – you've already got a full plate.

Staff development

Teachers need to understand the real dangers and risks that exist online, from cyber-bullying to sexting. The media frequently report stories of online grooming and radicalisation. Teachers should know what's out there and what students are up against.

CONSIDER: Set up an intranet or extranet e-safety site containing helpful articles you find online and elsewhere. This will make it easy for staff to find information.

Robust reporting

You must be able to respond right away to matters such as cyber-bullying or inappropriate behaviour. You should have a strategy in place that makes reporting easy, so that you can respond and intervene as soon as you know about it.

CONSIDER: Use another email address. Emails pertaining to e-safety will be sensitive. By using a different address, you can keep these emails separate from day-to-day emails. The account can be managed by the e-safety co-ordinator.

At the end of the day, e-safety is about people and their awareness.

geekpeek

Deploy email filtering solutions on exchange servers. You can monitor internal emails for inappropriate content, abusive language and bullying.

2. Encrypt it

Encryption is the most powerful tool for guarding sensitive data and personal details. By encrypting the data you hold, you're safeguarding its confidentiality against all unauthorised users – even if you're sending it over the internet.

Good encryption software protects data across multiple devices and operating systems. It encrypts sound, videos, DVDs, CDs, memory sticks – any data that can be stored on a device. Your encryption technology should be configured according to industry best practice. This doesn't just protect your students and staff, but your school or college as well. The Information Commissioner can issue fines for serious breaches of the data protection principles, so guard your data well.

Best practice tips

Make it easy on yourself. Follow best practice and you can prevent issues before they happen – just what your inner geek needs.

- Send only encrypted data over the internet
- Include encryption in your cloud security
- Ask your encryption software supplier about the algorithm. Does it align with international standards?
- Keep your encryption key in a secure location

- Keep a comprehensive log of every access to sensitive data – who accessed the data, why, and when
- Use a security solution that integrates with third-party applications

Create an encryption policy

This should be part of your institution's data protection policy. It doesn't have to be a 50-page document. Simplicity and clarity are key to bring everyone on board and must be reviewed regularly to ensure that it remains accurate. This is a good one to use as a guide:

Example

1. Introduction: This Encryption Policy is a sub-policy of the Information Security Policy (ISP-01) and sets out the principles and expectations of how and when information should be encrypted.

2. Definition: Encryption is the process of encoding, or scrambling, information so that it can only be converted back to its original form (known as decrypting) by someone with the correct decoding key.

3. When to use encryption: When sensitive or personal data is:

    - saved over data networks (Local Area Network or the Internet). This protects files containing sensitive information against the risk of interception and reading
    - accessed via network file shares or file servers
    - sent via email outside the institution or to unauthorised recipients within the institution
    - stored or accessed from mobile devices, such as laptops, tablets, smartphones, external hard drives, USB sticks, and digital recorders. Devices must use "full disk" encryption, no matter who owns the device
    - stored in public, cloud-based storage facilities to ensure that files are only decrypted by authorised users on authorised devices
    - subject to an agreement with an external organisation, the data should be handled (stored, transmitted or processed) in accordance with the organisation's specified encryption requirements and encrypted at all times while in transit to the external organisation

4. Key management: Encryption keys MUST be managed effectively and responsibly. Usually, access to encryption keys is through the use of passwords. If the encryption password is lost or forgotten, the encrypted information is rendered unusable. Some industry-leading solutions allow for audit-able key backup and restoration procedures.

Typically an institution will appoint a named Data Protection Officer. This officer is responsible for the Data Protection / Encryption policy. This person may nor may not be within the IT team, who are responsible for installation / enablement of the encryption solution.

5. Encryption standards: Only those who have been subject to substantial public review and which have proven to be effective should be used.

6. UK Law: Export regulations regarding cryptography (encryption) are complex, but so long as the encryption software is considered to be a "mass market" product you are unlikely to encounter problems leaving or re-entering the UK. Still, you may be required to decrypt any devices or files by UK authorities on leaving, entering or re-entering the country. If you are requested to decrypt your files or devices you should do so.

   Section 49 of the Regulation of Investigatory Powers Act (RIPA) includes a provision whereby certain "public authorities" (including, but not limited to, law enforcement agencies) can require the decryption of devices or files. Failure to comply with such a lawful request is a criminal offence in the UK.

7. TraveLLing abroad: In addition to the export regulations above, government agencies in any country may require you to decrypt your devices or files when you enter or leave the country. If you are travelling abroad with encrypted confidential data there is a risk that the data may have to be disclosed. You must consider the consequences of this. Wherever possible, do not take confidential data with you when you travel (keep the data at the school/college and access it using a secure, remote access facility).

   Pay particular attention to the possible inadvertent export of data subject to the Data Protection Act to countries outside of the EEA (or the few other countries deemed to have adequate levels of protection) when travelling.

3. Let's get social

Your inner geek is a powerhouse of superior knowledge. With that knowledge comes responsibility. With regular reminders, you can reinforce acceptable online behaviour for teachers and students alike.

This truly is another aspect of what makes you the school/college hero – by stopping the scarring effect of an ugly incident before it happens. And in the process, you can give yourself some much-needed breathing space.

Teachers should know...

1 Should teachers accept friend requests from students on their personal accounts?

Never. Yet a TES survey found that 9% of teachers were friends with their pupils on social media networks. Accepting requests – and thus, sharing their personal lives and information – makes teachers vulnerable. They're potentially leaving themselves open to allegations and exposing themselves to unwanted contact.

Teaching unions clearly state that friending pupils is inappropriate, but remind them by including this in your school/college e-safety policy.

The only time teachers should use Facebook and other social networking sites as a means to reaching out to students is through professional or organisational accounts, and always with their Senior Leadership Team's okay. They should also be aware that Facebook and other similar sites have a minimum age requirement of 13. Using professional accounts for anyone younger is just wrong.

2. Posting on a personal account

   Teachers are required to uphold the reputation of their institution. It is unacceptable to ever post negative comments about students, parents or colleagues.

3. That profile photo – is it okay?

   Our choice of a profile photo says something about us. Teachers should think twice and not give anyone any reason to doubt their professionalism.

Students should know...

1. Think before you post

   Before posting anything online, stop. If a teacher, parent or any authority figure that you respect saw your post, how would you feel? If the answer is 'uncomfortable' or 'ashamed', don't do it. Thanks to screen grabs, once it's online, it's there forever and can not be deleted.

2. Cyber-bullying

   Do not post replies to any unwanted message. Tell a parent or teacher. Together, you can decide your next move. Do not delete the messages either, as they can be used for evidence. (On the flip side, do not harass anyone online – it's a criminal offence.)

3. Set your profiles to private

   There's no reason for strangers to know about your life. It won't add to your popularity. The best way to stay safe online is to only allow people you accept or invite to see what you post.

4. Should you meet a stranger in person?

   Be on your guard. Flattery or even supportive messages might sound sincere, but it could be a way of manipulating you. Read between the lines before you decide to meet someone, either for friendship or romance. If you still decide to meet them, take a friend, tell a parent where you're going and remain in a public place.

5. Is your security software up to date?

   If it's not, you're allowing cyber criminals to steal your personal information. This can be used against you in a number of ways, and none of them good. Protect yourself with anti-virus software. Know what you're downloading. Bundles frequently include malicious malware, which can infect your computer.

geekpeek

Most network breaches originate from social media networks. Students click on links contained in friends' posts and just like that, they've put your network at risk. Keep your geek on and ensure you use content filtering to avoid problems. Sophos can help you with that too.

4. Prevent Duty

You need to follow government recommendations to meet the Prevent Duty. This is the government strategy to help stop students from either supporting terrorism or joining in extremist activities.

Don’t worry. Sophos makes this easy for you.

First things first. Ofsted’s revised common framework (1 September 2015) references the need for schools and colleges to have safeguarding arrangements in place. This echoes the statutory guidance on the Prevent Duty, which includes the need for institutions to keep students safe online from extremist material. You should make internet safety an integral part of your ICT curriculum. Weave it into Personal, Social, Health & Economics (PSHE) and Sex & Relationships Education (SRE). In fact, make it a part of your e-safety policy.

To safeguard students/young people, you can use specific systems and resources, such as Sophos Unified Threat Management (UTM).

1. Web Filter gives you 106 web categories. Criminal Activity includes data supplied by the Counter Terrorism Internet Referral Unit. You can block harmful material and also check reports for users, categories, sites, even URLs.

2. Internet Watch Foundation maintains a list of known criminal sites. As a member, Sophos adds IWF's continuous updates to the URL database and in turn updates UTMs, keeping you current.

3. Reduces the risk of malware being downloaded from legitimate or compromised sites, keeping students safe.

4. On-box reporting reveals search engine queries and gives you reports on individual user activity, so you can be proactive.

5. Can be integrated with YouTube, so you can set limits to what students can access.

6. Country clocking prevent users from accessing countries or regions that you specify.

7. Granular application control enables you to block, allow, shape and prioritise web applications with Deep Layer-7 inspection (Next-Generation Firewall). It identifies over 1300 applications, and you'll get feedback on unclassified applications too.

geekpeek

Students are going to try to use anonymising proxies to bypass your filtering systems. (That's what they do.) Sophos can help prevent these attempts, providing protection from harmful sites.

5. BYOD (Bring your own device)

Smartphones. Tablets. Everyone has something, and they're bringing it into schools and colleges, teacher and student alike.

Your inner geek has its work cut out. But that's what we're here for.
To make everything easy.

Let's start with teachers

You have a couple of options to protect data on BYODs. You can install containerization on tablets and mobile phones. This separates personal and work data. But it also affects performance, which will slow teachers down. The other option is to set security rules, such as password strength, and making sure built-in security is enabled. This is a decision you'll need to make with the Leadership Team.

If your school/college allows staff to use their own laptops, you'll need to assess the security settings before allowing it to connect to the network. You should also implement network access control for your network's protection.

Most of all, remember encryption. This must be used to protect personal information. (And by preventing a security breach, you protect your school or college's reputation and have one less worry.)

What about students?

There are so many pros to allowing students to bring their own devices into school/ college for educational reasons. The downside, of course, is that they can potentially access unsuitable material. Your network systems should be secure, and your filtering systems should also be able to block access to harmful sites, so no worries there.

While you're reviewing your e-safety policy, have another look at your BYOD directives. Your BYOD policy should cover:

Are you clear?

Make clear what your school's/college's expectations and responsibilities are. For example, students should understand that they can only use their phones and tablets with their teacher's permission, and only for learning purposes.

Do they agree?

Everyone must adhere to your Acceptable Use Agreement, which should be part of your e-safety policy. Be specific and leave nothing to interpretation. For instance, clearly state that they can not circulate videos and photos of other students.

Are they careful?

Students will keep their own login details private (username and password) and not share with anyone. They should understand that this prevents the device from being used if it falls into the wrong hands.

Are you trained?

All staff must undertake mandatory training in e-safety issues.

Are they trained?

Students should also receive training and guidance on e-safety issues. To make sure they apply what they learn, regularly monitor and audit their usage.

Is it lost or stolen?

If any device is lost or stolen – or if it changes ownership – students should report it. This should be part of your BYOD policy.

geekpeek

Sophos Mobile Control secures phones and tablets, letting you reinforce your policy. It can also protect data on devices with encryption, without slowing staff down.

6. What about cloud services?

Almost everyone's inner geek loves the cloud, with more and more schools and colleges headed this way. No matter where students are, or what device they're using, they can continue to learn and teachers can continue to work.

What a cloud service should give you

As the cloud is essentially a file server located on the internet, there are issues concerning the Data Protection Act, principle 8: data can not cross any borders without adequate protection.

So if the provider is based outside the EEA, they must participate in the self-certification scheme, which confirms their compliance with the Data Protection Act. The scheme also requires your cloud provider to give you useful advice, including how your school can best configure their cloud software solutions. If they can't do this, run. Run fast.

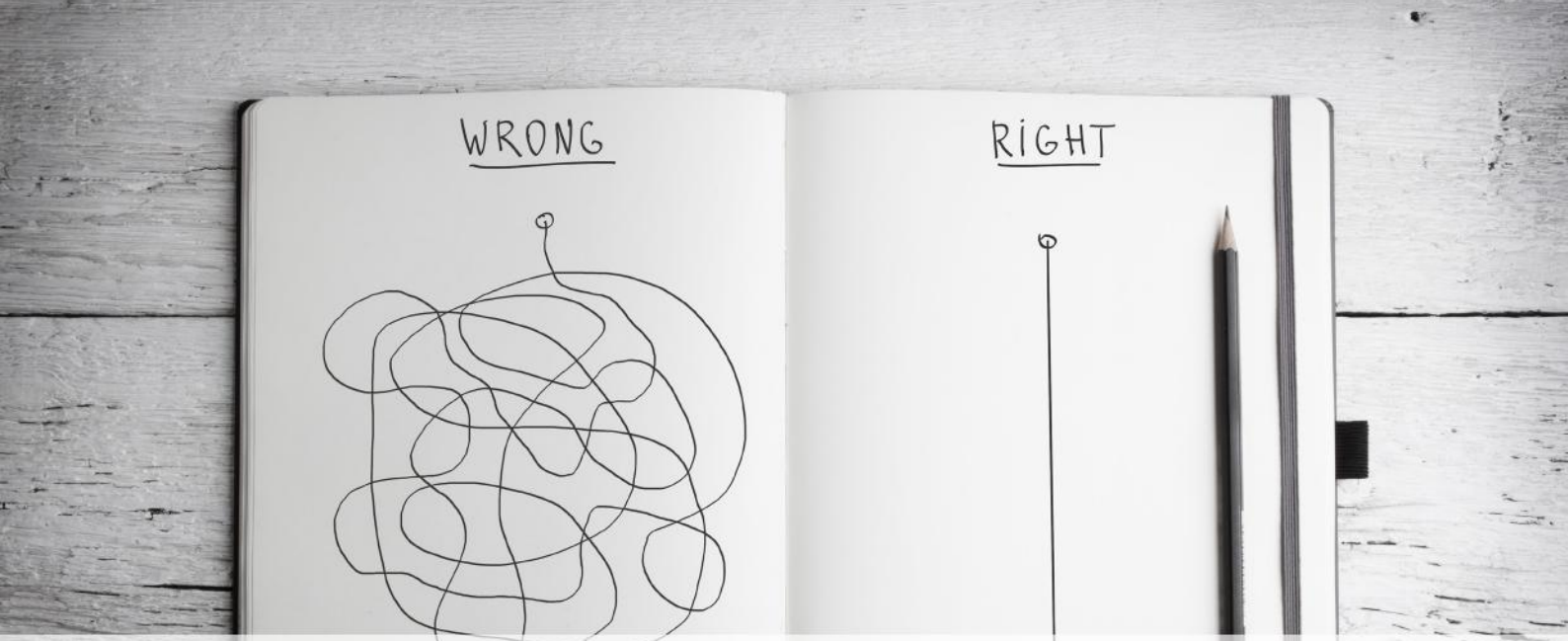
What about protection?

Sophos Cloud lets you manage students' learning experiences, while giving you the option to save on IT infrastructure. It's the only integrated and comprehensive security solution. We're talking about protection that goes where they go. You can manage endpoint security and mobile devices from one unified cloud console.

All stored data is encrypted and all applications are protected and running on secured operating systems. Sophos Cloud also gives you traffic insights and detailed event reporting, plus advanced threat protection.

geekpeek

Just about all of Sophos' security solutions are available in the cloud. It's a great option when your budget is tight.



7. Simplify your network security

Here's a great way to free up some time. Instead of using multiple layers of security from different providers, use one simple solution. Your inner geek will thank you for it. Your security will be easier to manage, and you don't have to worry about how people are accessing your network, no matter how involved your architecture.

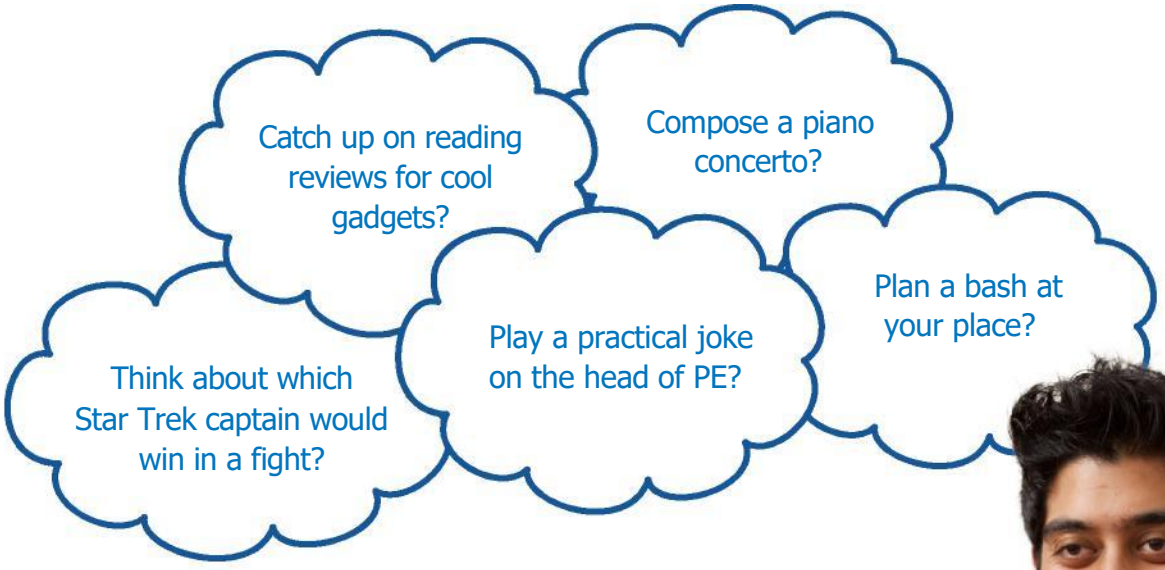
Sophos UTM is perfect for the job. It simplifies your IT security without the complexity of multiple-point solutions. We're talking about complete security from the network firewall to filtering and your servers in a single modular appliance. As your needs evolve, you can even add layers of protection.

This is the all-in-one approach, easy to install and manage at a price that will make you the hero of administration. Sophos UTM gives you:

- Consolidated network security platform – Intrusion Prevention Systems (IPS) allow us to monitor traffic and detect web-based attacks. Virtual Private Network (VPN) adds security to Wi-Fi hotspots and the internet. Together with email and web filtering, they combine with the industry's simplest admin interface, at the speeds you need. You can also choose the level of protection you need with modular subscriptions.

- ALL the Next-Gen FirewaLL features you need – Block, allow, shape and prioritise applications. Our Next-Generation Firewall gives you true application identification for over 600 applications. You'll also get automatic updates and feedback on unclassified applications.
- Intuitive management and detaiLed reporting – Know what your users are up to and get complete control over the features you need. Detailed reports give you the info you need to fix problems fast. Sophos UTM Manager lets you centrally administer multiple appliances through one single login.
- Connect remote offices with VPN and Wi-Fi – Free up your staff. Sophos RED (Remote Ethernet Device) doesn't require any technical skills at the remote site and forwards traffic to the UTM for complete security. Sophos UTM also works as a wireless controller; access points are automatically set up and receive complete UTM protection.
- Free security appLications – Our Linux-based OS includes a free Essential Network Firewall. You'll get fundamental security like firewalling, networking tools, routing and secure remote access.

What can you do with your extra time?



geekpeek

With Sophos UTM, you can install on your platform of choice: hardware, software, virtual or even in the cloud.

8. Stop Advanced Persistent Threats

All it takes is for a student or teacher to click a link or share personal identifiable information on social media, and just like that, a hacker is in.

Most security solutions can't stop it from happening. They're simply not programmed to find these vulnerabilities. And if they don't know about them, they can't act.

Life is never easy for a Network Manager. But here's what you can do.

1. Arm yourself with knowledge

The more you know, the better prepared you are. Sophisticated hackers – also known as "Advanced Persistent Threat actors" – consider schools and colleges easy prey. Typically, the threat looks like this:

Target

Hackers decide on the site they're going to target.

Plan

They do extensive research to find vulnerabilities before launching the attack. These people are usually well funded and organised.

Stealth

They gain access to your network through an unsuspecting user. They'll then move further into your network looking for anyone who's authorised to access higher-value systems. This could be you or your head.

Lie and wait

Sophisticated threats like APTs want to avoid detection, so they'll do nothing at first. They can be dormant for days, weeks and even years, giving them time to fortify their attack.

Extract data

It then communicates with the command and control (C&C) host for instructions and begins extracting data.

That's it in a nutshell. The question is, what do you do about it?

2. Arm yourself with Sophos

Sophos Malicious Traffic Detection

You can get the upper hand with Sophos Malicious Traffic Detection (MTD). It monitors your traffic and will know immediately if a connection is being made to websites associated with malware delivery. MTD will kill it and remove the underlying software, keeping your data safe and sound.

Sophos Sandstorm

There's still dangerous, unknown malware out there. Sophos Sandstorm uses advanced cloud-based technology to detect unfamiliar files, isolating and analysing them to determine if they're safe. Your protection is entirely visible with detailed, incident-based reports.

Sophos UTM

Heartbeat is part of the Sophos UTM, which gives you a government accredited firewall. It includes Intrusion Prevention to check for malevolent activity coming into your network. Web filtering blocks dodgy websites, while Webserver protection stops unauthorised users from accessing publicly available internal servers.

Email filtering prevents spam and malicious emails and the Wi-Fi controller keeps your wireless network under control and shielded from those wanting to use your network.

Sophos Heartbeat

Heartbeat is synchronised security. Sophos Enpdoint communicates with the UTM so that it can see what's happening on the Endpoint device. If it notices something wrong it can prevent the Endpoint from communicating externally. No time is wasted finding the problem, because we know where it is. We fix it and share the information across your network so that we can instantly see if the malicious malware is hiding anywhere else.

Ransomware and what you can do

We've written a really helpful blog on Sophos Naked Security. It's the story of good vs. bad, and it's definitely worth reading: "Security vs. convenience: the story of ransomware spread by spam and email". Here's the link:

https://nakedsecurity.sophos.com/2016/03/14/security-vs-convenience-the-storyof-ransomware-spread-by-spam-email/

3. Arm them with education

Keep kids and staff educated on these threats. Include this information in your school or college's safeguarding policy. You can also use "The Little Big Book of Badness", which we've put together to enlighten younger students on what to look out for. You can check it out at www.sophos.com/LBBB

geekpeek

It's not unusual for tech-savvy students to try and breach your network to flex their skills. Sophos UTM makes their attempts an epic fail.

9. Speak their Language

This, or something like it, is probably part of your job description:

Advise leadership team, teachers, support staff and students on the use of software and hardware, including technical and specialist information.

How many do you think actually understand what you're talking about? If you're using tech talk, you might notice their eyes glaze over. The result is frustration for you and them. Here's how to make yourself understood so that everyone gets what they want: they know what needs to be done and how to do it, and you can step back and put your feet up for a change.

Talk about actions, not systems

Relate to them. Explain it from their point of view. Tell them what the technology does, not necessarily how the code or system works. The results are what they're interested in; the process of how it will happen – unless that's relevant – isn't what they want to know. You've got to walk a fine line here. You don't want to talk down to people. You just want to make it easy to understand.

Metaphors can help

Try saying this to someone: "The notional environment in which communication over computer networks occurs."

No one will know what you're talking about. But use the metaphor – cyberspace – and now they're on board. You can explain that web infrastructure works like (use your imagination). Actually, your English teachers would tell you that's not a metaphor. It's a simile. (See? We can't all be experts at everything). The point is, by putting something in a context, you can give them an 'aha!' moment. They'll get it.

The danger is that you can oversimplify something – just make sure they arrive at the correct conclusion.

Feel their pain

Put yourself in their place. We've all encountered situations where we feel out of our depths. Feeling clueless is never pleasant, and for them, talking to you is probably one of those experiences. Remember humility. Understand where they're coming from and hopefully, that will give you patience. Don't let the conversation end until they get it. Otherwise, they'll walk away even more frustrated.

geekpeek

Use visual tools. Diagrams help people understand what you're talking about. Draw it if you have to. Videos are also good. If you're using a Sophos solution, we probably have a video that explains it.

www.sophos.com/videos

10. Consolidate security products

As budgets are squeezed, Heads need to see Return on Investment. This can be achieved by reducing the number of different companies you use for your security products.

Using multiple IT security solutions from various vendors consumes more time than you have. And then patching is needed to help products work together. One consolidated solution simplifies the process, taking care of all risks. It also means you'll spend less time managing your security, so you can take care of other matters on your 'to do' list.

Why one vendor?

Here's how to make your Head Teacher love you even

more: Cost savings:

Schools and colleges must cut costs and improve return on investment, and this is a smart way to do it.

Time savings:

All you have to do is implement one solution.

Increased buying power:

You'll improve economies of scale. By leveraging one vendor, you can get more for less.

Reduced training requirements:

Think how much simpler training new staff will be. It also means everyone is working from the same page. Knowledge transfer is easier.

One familiar interface:

Less stress if someone's off sick. Also means your team can be more productive.

Less administration and fewer meetings:

Partnering with only one vendor eliminates multiple meetings, paperwork and contracts.

Less risk:

One consolidated solution covers everything and every risk. Multiple solutions can leave holes in your security.

One support desk:

If you need support, you have just one number to call.

geekpeek

Sophos can help you get the most for your money with a fantastic range of solutions and ideas—by consolidating!

Class Networks are a registered Sophos Solutions Partner and specialists in providing, network, telephony, mobile and cyber security solutions to the voluntary and charitable sectors.

Call 0800 160 1920 or email contact@classnetworks.com to discuss your

CLASS NETWORKS