Cyber, IT and Technology FAQs

In partnership with Nick Hawkins, Director of Global Secure Accreditation (GSA)

BTA | BUSINESS TRAVEL ASSOCIATION

Join the Conversation: #yourbta #btaupdate #strongertogether

Contents

01

Dear Members & Partners,

In this latest FAQ guide, we are looking at another key area to ensure you are best equipped to face the current situation.

Despite lockdown and the uncertainty of what a "new normal" might look like, today's increasingly connected world means we can go on with most of our professional and personal lives virtually. However, with a huge increase in the number of people working remotely, it is of critical importance that we take care of our cyber environment.

This week, Nick Hawkins who left the Police Service in 1990 and has subsequently developed his career in the technology sector as a Director at our valued partner, Global Secure Accreditation, has sat down with us to impart some invaluable advice on how to create the safest and most secure set-up whilst working from home.

GSA is the world's first truly independent system of hotel security accreditation, established and operated by highly experienced security experts and created in partnership with SFJ Awards (SFJ) - a UK Government (Ofqual) approved standards awarded organisation. The Global Secure Accreditation team is made up of highly experienced former law enforcement practitioners, UK military, UK Counter Terrorism and international security experts, bound together by a common desire to set the highest professional standards.
In the following pages, we will go through top tips on Cyber Security; be it about passwords, VPN, Firewalls, updates and scams, alongside what you could be needing as employers on platforms you use to communicate and share information or to back-up your data; and how to manage security as an employee, whether it's securing your home Wi-Fi or your devices, protecting yourself from scams and ensuring your privacy while working from home.

With this information, we want you to feel reassured and comfortable when working remotely.

I want to thank all the amazing companies and people who are partnering with us and lending us both their time and expertise to bring you valuable information, advice and support as we continue to evolve this series. As ever, we would love to hear from you what you would find useful.

With this initiative, alongside our campaigning work, we can help shape the industry whilst supporting each other.

I cannot say it enough, the BTA is here to support you all!

Thank you for your loyalty and take care.
Best wishes,

Clive Wratten
CEO, The BTA

Top 10 Tips For Everyone

10 Top Tips for Everyone

03

FAQs

A Quick How to Guide

How do we remember lots of passwords?

Create a short phrase regarding the service you are logging into, that will stick in your head. Come up with a phrase that can be tailored to any number of sites, this becomes your passphrase rather than a standard password.

How do you set-up a firewall at home? What does it do?

Click on the Start menu and type windows firewall in the search box. Pick the "Windows Firewall" option that pops up in the search results. If you're on Windows XP, hit the Run option and type in firewall.cpl. in the left sidebar, click "Turn Windows Firewall On or Off".

What is the best antivirus software and where should I get it from?

Having one of the best antivirus packages installed remains a necessity, particularly considering current world events. There are many familiar names such as Norton, McAfee and AVG along with both premium and free antivirus applications. A recent 2020 survey by Techradar recommended the following top 5 antivirus products: Bitdefender, Norton, Kaspersky, Trend Micro and Webroot.

How do you secure a home router?

The main thing you can do is change the default admin password. Many routers come with default administrator passwords and attackers constantly try to break into devices using these publicly known credentials. After you connect to the router's management interface for the first time through your browser, the address should be the router's default IP address found on its bottom sticker or found in the set-up guide. Make sure the first thing you do is change the password.

What are remote desktop tools and how do I avoid them?

Windows Remote Desktop allows others to connect to your computer remotely over a network connection, effectively accessing everything on your computer as if you are directly connected to it. When you don't need the Windows Remote Desktop feature, turn it off to protect your computer from hackers. Type "remote settings" in the Cortana search box and select "Allow remote access to your computer".

03

FAQs

A Quick How to Guide

What are encrypted communications?

Encryption is essential for securing data, either in transit or stored on devices. It can provide peace of mind that communications will not be intercepted, and that sensitive information stored on devices can't be exfiltrated in the event of loss or theft.

How do I make sure I am running the latest versions?

In addition to fixing security flaws, updates also come in the form of bug fixes and new features, both of which are nice to have. There are three major areas of your PC to keep up to date:

Windows Windows Update has grown more insistent over the years in keeping itself up to date. In Windows 10, security updates are downloaded and installed automatically. You don't get a choice in the matter.

Third-Party Apps Keeping third-party apps up to date is nearly as important as keeping Windows itself updated.

Unfortunately, how updates get installed is up to the people making those apps. Fortunately, there are some tools out there that can help you make the process a bit easier e.g: Patch my PC.

Hardware Drivers By and large, keeping hardware drivers up to date is less a security issue than one of functionality. New driver updates tend to add bug and stability fixes or, in the case of things like video card drivers, better performance and functionality with newer games and apps.

What is a VPN and how do I get one?

A VPN is a Virtual Private Network. We recommend that people download a VPN from their anti-virus software providers for their devices whilst working from home. This is an extra layer of security for your devices and all data that is shared from them.

04

FAQs

Employers' Questions

How safe are the platforms such as Teams, Zoom, Hangouts? Is there one that stands out as the safest? Or the most technologically advanced?

The Webex video conference platform has been around since 1995 and is a favourite of the privacy-conscious health care, information technology, and financial services industries.

This is partially because all three industries commonly relied on virtual meetings well before the Covid-19 pandemic, but mostly because Webex has a reputation for maintaining robust cybersecurity. Cisco, its parent company, is an industry leader in network hardware, software, and security products. Webex offers end-to-end encryption but has had security issues in the past.

Microsoft Teams experienced an uptick in the recent crisis, in part due to its integration with the company's flagship Office365 cloud and productivity services. Teams is encrypted "in transit and at rest," but details about support for end-to-end encryption are vague.

One advantage of Teams is that its parent company is a major provider of networking, software, and cybersecurity services.

Microsoft has an internal rating system for the security of its products which means that it can adhere to the strictest government and industry security standards and legal requirements.

Neither Microsoft nor Teams are immune to security vulnerabilities, but as a company, Microsoft's bandwidth to address them when they occur is probably unparalleled. Microsoft also has a more transparent privacy policy and a better track record when it comes to protecting user and customer data than many of its competitors, including Zoom.

Google offers **Hangouts** and **Duo** as its two primary video meeting platforms - both offer "free" and paid versions bundled in with its G Suite line of applications.

While Google Hangouts offers similar functionality to Zoom, it has a limit of 25 attendees per video conference. Other considerations include a long history of security and privacy concerns and the fact that Google Hangouts doesn't offer end-to-end encryption. Duo is end-to-end encrypted and can support video meetings with up to 12 attendees.

04

FAQs

Employers' Questions (cont.)

Like Cisco and Microsoft, Google has more resources dedicated to cybersecurity, but the company has a lengthy track record of mining user data, especially for "free" services. The company is also notorious for quickly and unceremoniously dropping support for many of its projects and has done so with several previous video conferencing and meeting apps.

Zoom's rapid increase in popularity in an already crowded market is a testament to its many qualities, features, and ease of use. The company has made some misleading claims about user privacy and data, and the recent discovery of multiple serious security vulnerabilities will test the company's ability to support and sustain its user base.

A good sign is that Zoom announced a 90-day freeze on any new features so it can focus on security and privacy issues. This move could help the platform and the company to continue the meteoric rise in the number of people using the service.

For industries with stringent data privacy and security requirements, platforms like Webex or Microsoft Teams may be a better fit, but it's essential to be mindful that every company, platform, and technology has its own set of drawbacks and vulnerabilities.

What is the safest way to back-up data with all my team working from home?

Unfortunately, there isn't a single answer, because people have different amounts, different types of data and different needs. Working from home is great but it comes with great responsibility for each individual and you want to make sure personal information is secure and data doesn't get compromised. If you stay connected to a Virtual Private Network (VPN), it's nearly impossible for your data to ever come under attack.

Storing data back-ups at an off-site location is probably the best way to ensure that a copy of data will remain sheltered from any event that may befall a business. A mature cloud storage provider that has a good track record for reliability will help ensure that your data is available when you need it. Some cloud services use innovative storage techniques to yield lower storage and operational costs.

04

FAQs

Employers' Questions

What can I do if I am suspicious of something not being secure?

The simple message is don't continue with the action you are undertaking and report the matter to your IT team. Make sure your devices and software are fully up to date with software and security patches.

Is there a way to (legally) check that my team are working and keeping data backed-up?

Monitoring and assessing the performance of people who work at home is perhaps the most significant managerial challenge. It can be helpful to measure their effectiveness in terms of their output rather than the hours they work. Agree set goals and deadlines for tasks. Keep a close eye on how well the targets are being met and give feedback promptly and sensitively if things go wrong.

As for data back-ups these can be automated. If you want to track an employees' WFH activity, first off let employees know they are being tracked and how, e.g. through a software application.

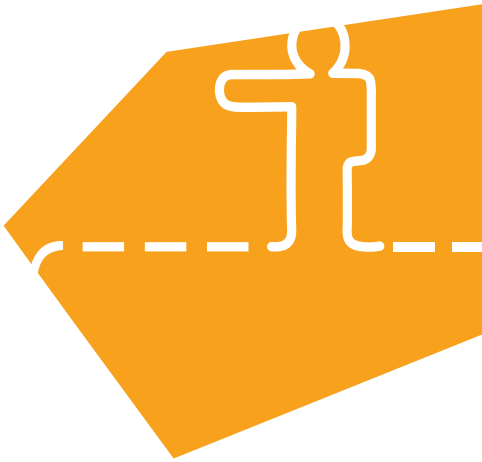
How can you get around all of your employees being on different Wi-Fi systems?

Are there specific things I must insist on?

(a) Make sure your colleagues have access to your organisation's cloud infrastructure and can tunnel in through a VPN with encryption.

(b) Ensure their home Wi-Fi has a strong password, in case a VPN isn't an option, or if it fails for some reason.

(c) Access to the settings on a home router should be password protected as well. Be sure to change the default password it came with to a strong password.



05

FAQs

Employees' Questions

What phishing scams should I be looking out for?

Fake lockdown fines People have been warned not to fall for a bogus text message saying they have been fined for stepping outside during the coronavirus lockdown. The scam message claims to be from the Government, telling the recipient their movements have been monitored through their phone and they must pay a fine or face a more severe penalty.

HMRC goodwill payment The MET police are warning of a fake message designed to steal your account details that says: "As part of the NHS promise to battle the COV-19 virus, HMRC has issued a payment of £258 as a goodwill payment."

Free school meals The Department for Education has issued warnings about a scam email designed to steal your bank details saying: "As schools will be closing, if you're entitled to free school meals, please send your bank details and we'll make sure you're supported."

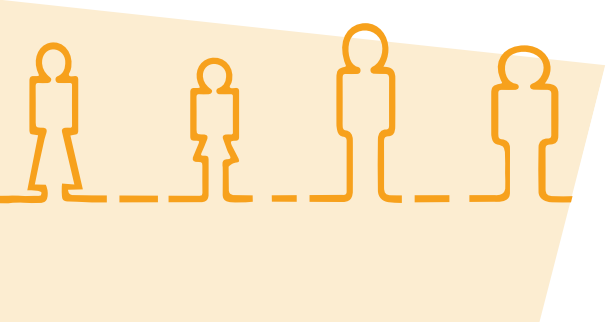
WhatsApp request to forward your code
A recent scam could grant hackers full access to your WhatsApp messages, photos and videos. Someone who knows your phone number could request to register your WhatsApp on a different device, and when a verification code is sent to you, the hacker will then message you to try and coax you into forwarding this onto them. They could then target your contacts with requests for money.

How can I ensure that my home Wi-Fi is secure and I am protected at home?

(a) Secure your home Wi-Fi with a strong password.

(b) Access to the settings on your home router should be password protected as well. Be sure to change the default password it came with to a strong password and not 12345 or Password.

(c) The enhanced online privacy provided by a VPN is also a reason for considering the use of a VPN for your devices at home even when you are not on public Wi-Fi.



05

FAQs

Employees' Questions

Is this the same as Work from Home scams in the news?

They are in the sense looking to fraudulently obtain information, but with a different strategy. Work from Home scams in the news are online job scams that take advantage of job seekers in a variety of ways. Scammers have several purposes, depending on the scam—to collect confidential information to use for identity theft, to get you to cash fraudulent cheques or send money, and to get you to pay for services or supplies, fraudulently.

Can my employer demand that I upgrade my home Wi-Fi?

Employers are recommended to provide telecommuting workers with equipment that they need to do their jobs efficiently and confidentially. Part of that can be to reimburse you part of your Internet costs.

How can I protect my personal devices as well as my work ones at the moment?

Make sure your devices and software are fully up to date with software and security patches and switch off or make sure they are secure when leaving them unattended. Also, criminals know there are extra laptops, tablets and smartphones to steal, so make sure all devices have full disc encryption enabled.

Can my employer see what I am doing now that we are working from home?

As a rule of thumb, I say the answer is "yes". It is always possible that logging software is installed that could potentially monitor everything you do on a work device. Although it all sounds a little covert, in reality, employee monitoring in some form or another is acceptable and indeed expected in most circumstances. There are numerous reasons for employers wanting to keep tabs, including improving employee safety, increasing productivity, and guarding trade secrets.

06

Summary

From Nick Hawkins

For many of us, working at home some of the time, is a bonus. But for the foreseeable future, with the potential of home-schooling children at the same time, the novelty will soon wear off.

For others this maybe the first time they have been issued a work laptop or other device for remote working.

We will likely see an increase in the number of cyber-attacks and scams against corporations and individuals over the coming weeks and months, with cyber criminals seeking to take advantage of the COVID-19 pandemic. It is vital to bring the awareness level of employers and employees up as fast as possible along with implementing simple actions to protect themselves .

We are also seeing many organisations in the cyber security community sharing resources and removing the cost of some of their products to help at this difficult time. It's a great opportunity to implement some of the security layers to protect yourselves.

Best wishes,

Nick Hawkins
Partner, Global Secure Accreditation

External Resources

General Coronavirus links

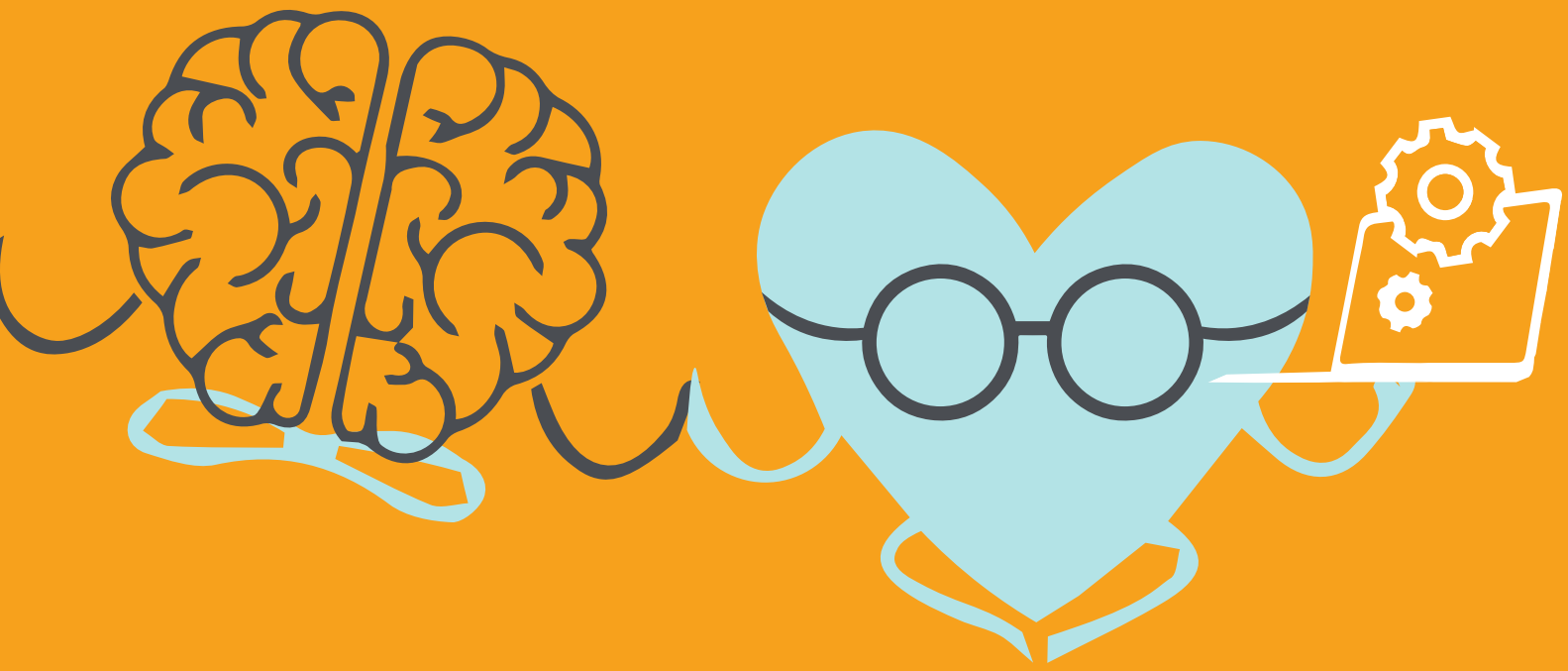
Public Health England www.gov.uk/government/organisations/public-health-england

NHS UK: www.gov.uk/government/collections/coronavirus-covid-19-list-of-guidance

Places that need volunteers or online help

NHS Volunteer Responder: www.goodsamapp.org/NHS

Samaritans Online Chat portal: www.samaritans.org/chatdonate/



BTA | BUSINESS TRAVEL ASSOCIATION

Designed by
Pembroke and Rye