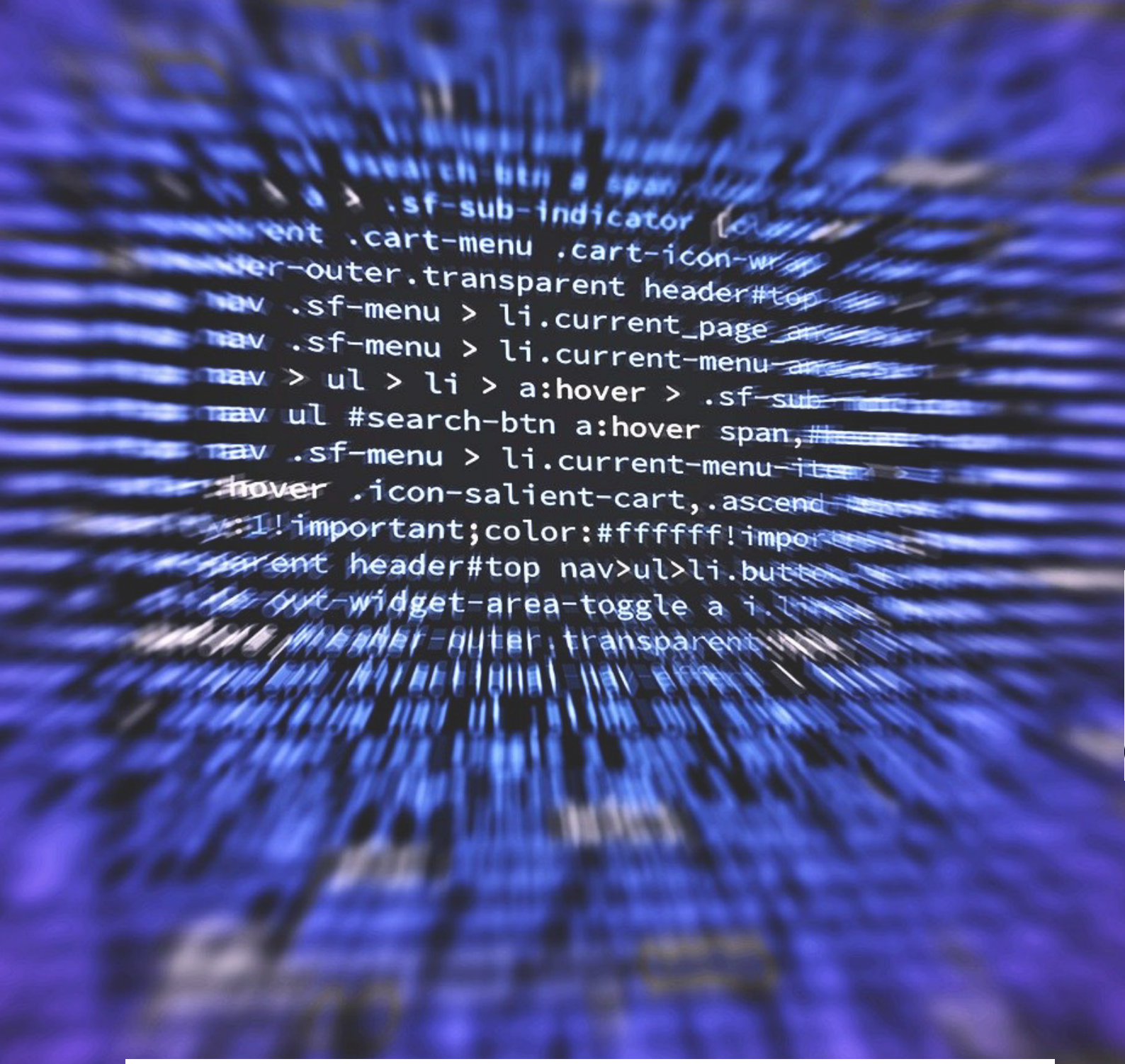


# STAYING CYBER SAFE

## when working from home

gfirst LEP
growing gloucestershire

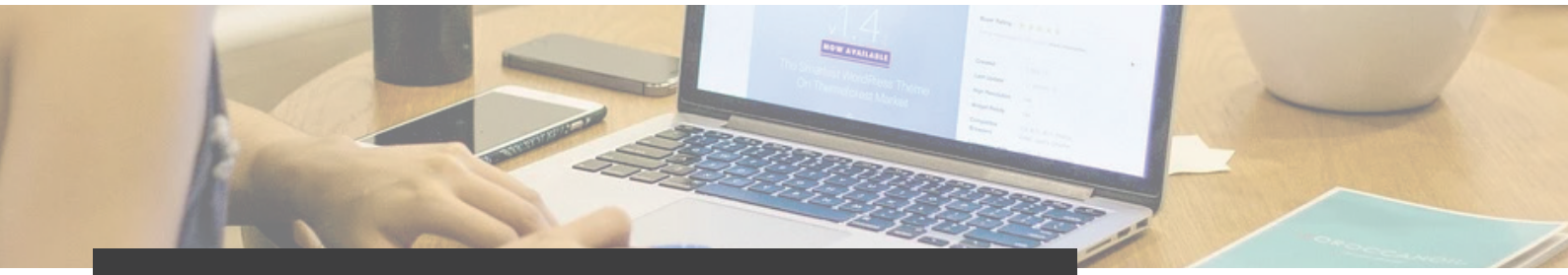
CYBERSECURITY Associates

# AN EXPERT GUIDE TO STAYING CYBER SAFE

## when working from home

As we prepare for possible restrictions to business activities and encourage more home working, it is important to remember that cyber attacks are still a potential threat. In fact, cyber attackers may see the coronavirus outbreak as an opportunity to increase the frequency and severity of cyber hacking.

This emergency guide to staying cyber safe when working remotely can help both businesses and employees to prepare and defend against cyber threats.



# TOP TIPS FOR IT SAFETY

## Laptops & Tablets

Some larger businesses may provide home workers with laptops or tablets; however, many employees will have to rely on using their own devices. Make sure you have the following in place:

- A good anti-virus product. We recommend Windows Defender, which is free to install, or AppGuard, which defends against ALL types of malware including ransomware.

- Check that your anti-virus programme is up to date and has the latest updates installed. Some products will do this automatically, but some will require manual updates.

- Ensure device encryption is enabled on your laptops. This feature is designed to protect your data from unauthorised access. Windows 10 comes with encryption features, so make sure these are enabled.

- If using business IT, enable all security controls. It is also worth considering cyber monitoring.

# Home Routers

Your home router or broadband allows you to connect to the internet when working from home. Therefore, it is vitally important that these are looked after, otherwise your private data, home network and everything connected to it may be at risk.

Keep your router secure and separate out the access between home usage and work usage – follow the steps below:

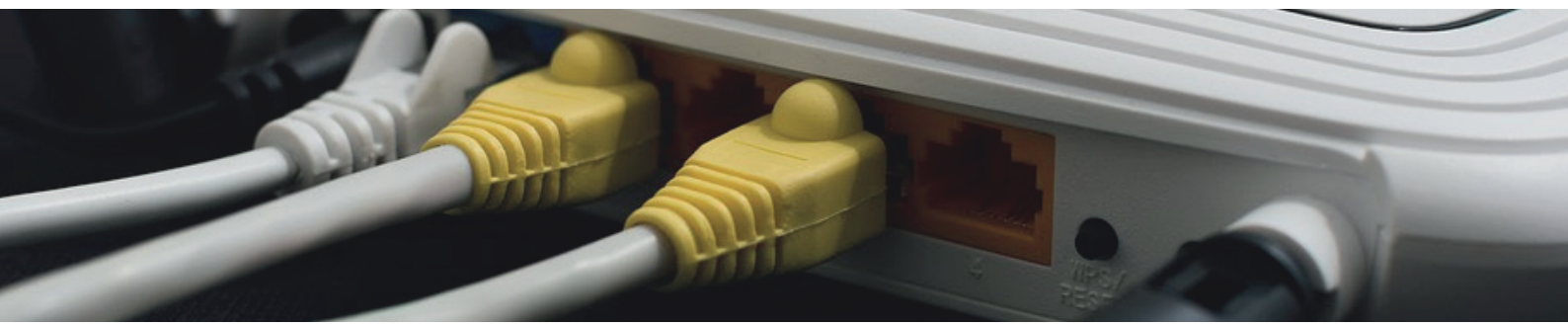
- **Change the admin login.**
  Your admin login and wi-fi password are printed on the back of the router – therefore, anyone could access your whole home network. Log in to your router as an admin and change the password to something complex and strong.

- **Change your router name.**
  It is easy for cyber attackers to identify a router's make and model, and gain access by exploiting vulnerabilities. You will make the cyber attacker's job much harder if you log in as an admin and change the name of your router.

- **Enable a guest network.**
  Consider setting up a separate guest network and connect to this with all your home devices. You can give your friends and family access to this guest network. This keeps your work network separate and protected in case the home network is hacked.

- **Monitor attached devices.**
  Log in as an admin and check how many devices are connected to your wi-fi network, and which devices they are. It is always good to be aware of who is connected – after all, you don't want your neighbours benefiting from your wi-fi!

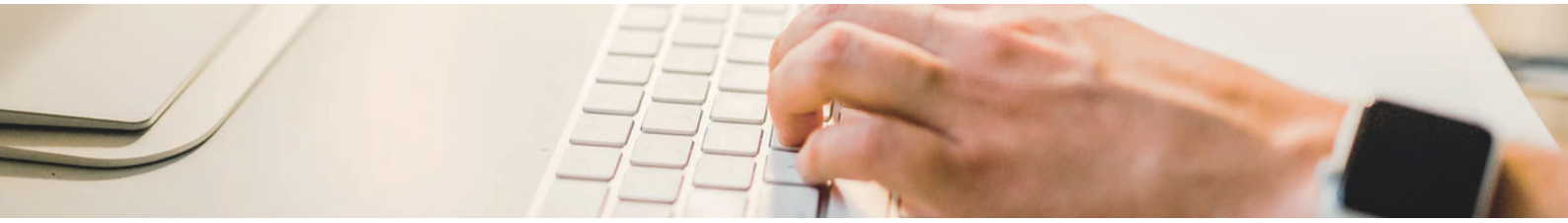
- **Regularly change your passwords.**
  Ensure you change your router/wi-fi password on a regular basis to something complex and strong.



# Beware the Bogus Email!

When working from home, we rely heavily on email to communicate with colleagues, suppliers and customers. Cyber attackers can exploit this by pretending to be someone else by using a credible-looking message.

Example: The cyber attacker could impersonate somebody from your IT team who asks you to open a document. In order to open the document, you must enter your username and password.



**TOP TIP**

**Nobody should EVER be asking for your username and password. If this happens, you should contact your Line Manager or IT team for assistance.**

# Working Together

Just because working from home involves individual working, that doesn't mean you should stop working together as a team. The cyber attacker may attempt to exploit your isolation, applying pressure on you to share information or interact with him. Double check any actions that you are suspicious of with your colleagues or Line Manager.

**TOP TIP**

**Don't solely rely on email to communicate with your team. Try using phone calls or video conferencing to communicate aswell.**

# Fast Response

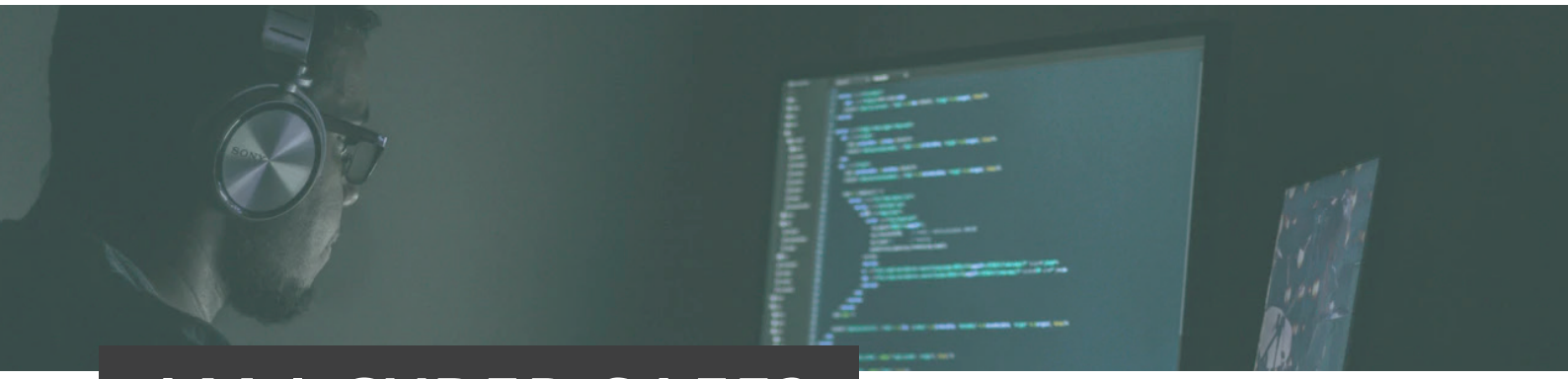
Like physical viruses, a computer virus can spread quickly unless it is contained and killed. When working from home, make sure you understand who needs to be informed if you suspect you have been cyber attacked. Most businesses have an incident reporting process – but if in doubt, contact your Line Manager.

**TOP TIP**

**Keep your work contacts up to date with phone numbers and email addresses. Your IT could be out of action following an attack, so it is important to ensure you can still contact your colleagues.**

**TOP TIP**

**Keep back-ups of all documents and information you use for business purposes. Consider a cloud back-up or an external hard drive.**



# AM I CYBER SAFE?

| QUESTION | BUSINESS IT | HOME IT |
|---|---|---|
| What IT is being used for remote working? | | |
| Is my device encrypted? * | YES ☐ NO ☐ | YES ☐ NO ☐ |
| Is my information backed-up? | YES ☐ NO ☐ | YES ☐ NO ☐ |
| Do I have anti-virus installed? | YES ☐ NO ☐ | YES ☐ NO ☐ |
| Are my anti-virus and operating systems up to date? | YES ☐ NO ☐ | YES ☐ NO ☐ |
| Is my information backed up? | YES ☐ NO ☐ | YES ☐ NO ☐ |

*check with IT team for business, and security settings for own IT

# FURTHER INFORMATION

## HOW AM I CONNECTING TO THE BUSINESS NETWORK?

(wi-fi router, hot spot, Virtual Private Network etc.)

## IS MY HOME NETWORK SECURE?

(check router name, change passwords, create guest network, etc.)

## DO I KNOW THE INCIDENT RESPONSE PROCESS?

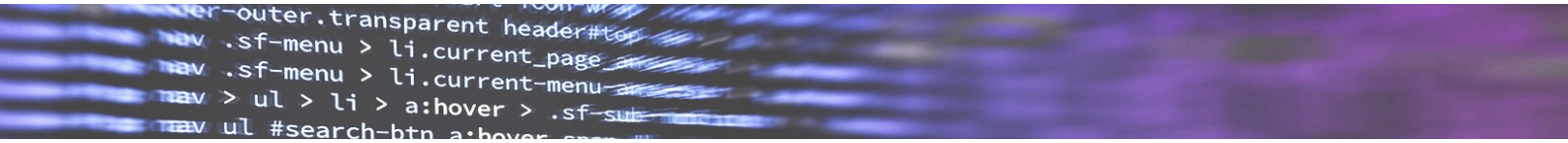
(if not, check with your Line Manager or IT Team)

## ANY OTHER NOTES?

# STAYING CYBER SAFE

when working from home

by CYBERSECURITY Associates




## YOUR EXPERT INFORMATION SECURITY PARTNER

Cyber Security Associates (CSA) provides expert cyber and information security services to UK FTSE 100 companies and SMEs globally.

**Managed services | Threat monitoring | Crisis response**
**Cyber security assessments | Response and recovery**
**Threat detection and protection | Cyber in education | and more**

Find out more at
**WWW.CSA.LIMITED**

CYBERSECURITY Associates