RSA INSURANCE

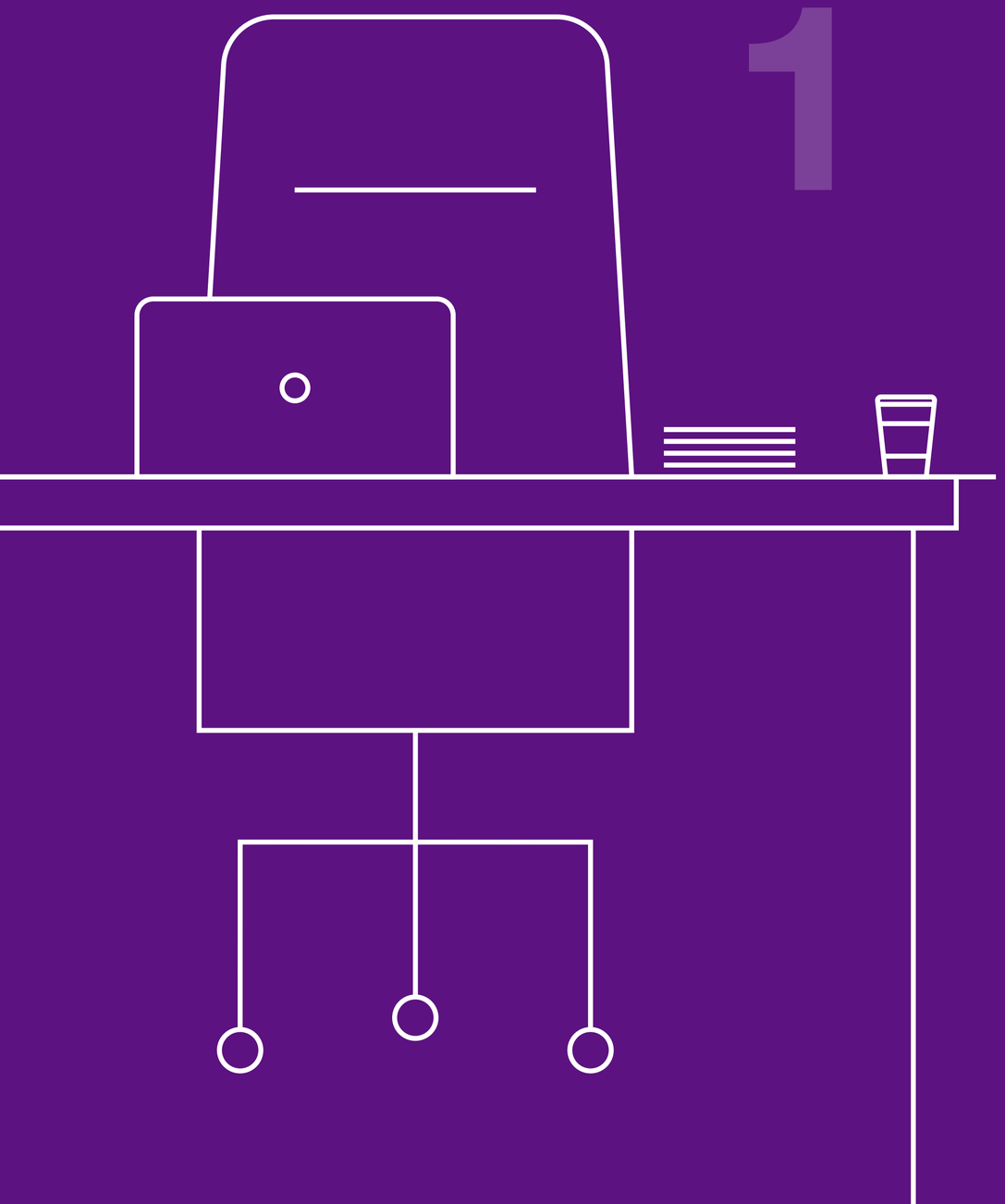
10 tips for success

Stay secure at home or back at work

The benefits of working from home for both organisations and employees have been embraced globally throughout the Covid19 pandemic...

...and arguably it has changed the way that many companies operate for the future. With increased home working and therefore a greater reliance on technology, cybercriminals are exploiting the current situation for their own gain. As the possibility of moving towards a more remote way of working is probably here to stay, it is more important than ever that we are aware of cyber risks that are present not just at home but wherever we are working.

It goes without saying that any operational disruption, for example, a cyber incident can be devastating for both businesses and their customers. With this in mind, we have put together some helpful guidance to help you stay safe whether you're at home or returning to work.

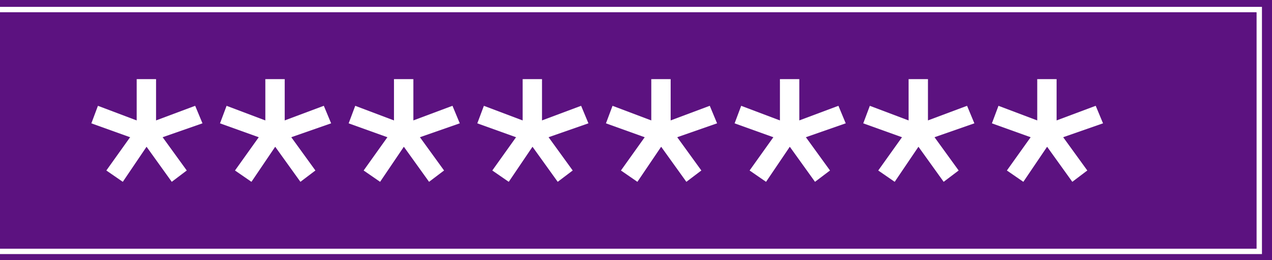


1

Identify and secure your physical workspace.

Find a space that allows you to maximise your productivity. Ensure you use a clean desk policy where you secure work-related items like printed material or devices when not in use, or shred important documents you no longer need.

2



Set unique, strong passwords and don’t share them.

Also consider a password management tool – an app for your phone, tablet or computer that stores your passwords securely, so you don’t need to remember them all.

3

Secure your tablets and devices.

Use a screen lock for that added layer of security.

4

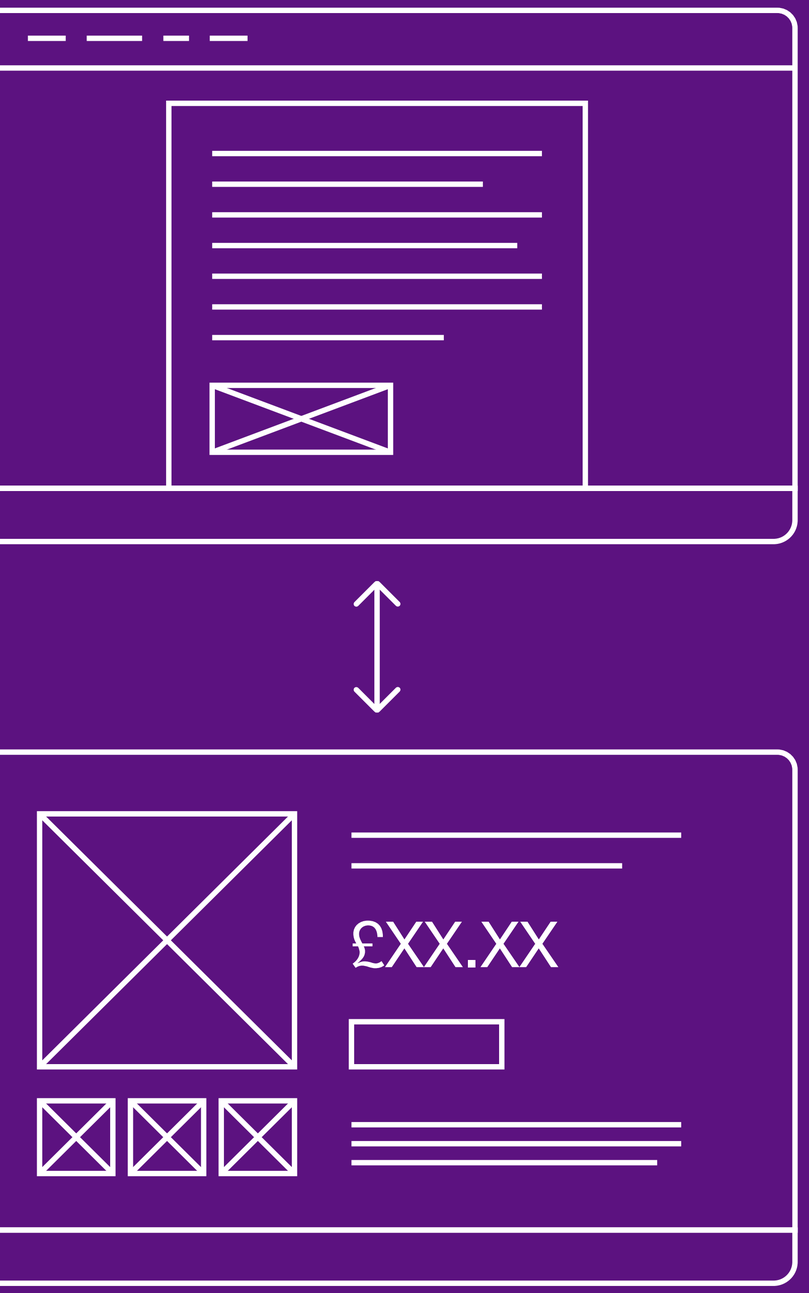
Keep your software and apps up-to-date to ensure you are fully protected.

Cyber criminals use weaknesses in software and apps to attack your devices and steal information. Software and app updates are designed to fix these weaknesses and installing them as soon as possible will keep your devices secure.

5

Know your organisation’s policies, procedures and expectations.

When working away from the office in a new, flexible working environment, it is likely you will be travelling between different locations with your work devices a lot more - ensure all confidential data is encrypted, review all of the appropriate guidelines and know who to ask for assistance or clarification.



6

Keep your work and personal life separate.

Don’t use your work device for personal activities and never use the same passwords across work and personal accounts. If one gets compromised, they both do.

7

Be aware when using any devices in public.

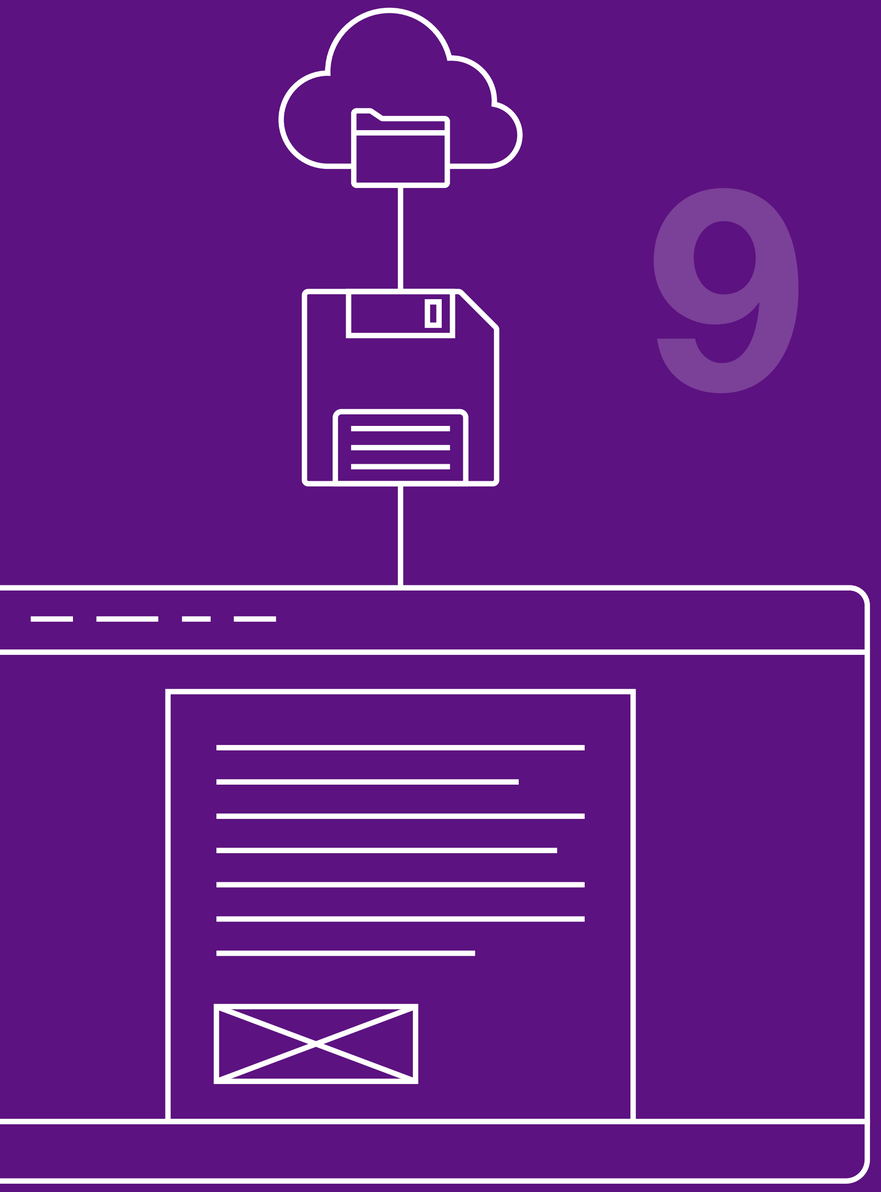
The security threats around you are much greater when you are away from your home or the office. Stay alert to your surroundings and don’t take any unnecessary risks.

8

Make sure your internet connection is secure wherever you are working.

One of the biggest security holes working away from the office is the internet connection.

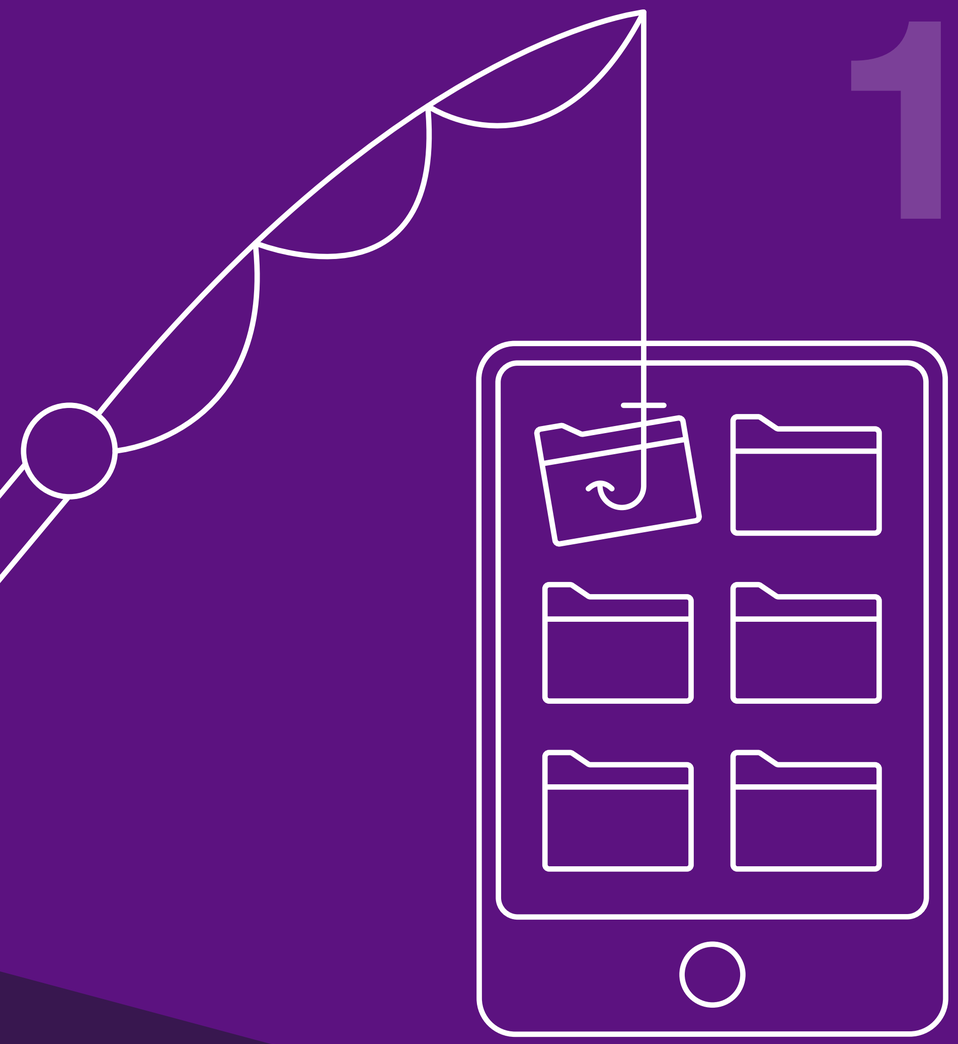
- If you are working from home, change the default password and enable the security settings on your router
- Where available, ensure you use VPN technology every time you are connected to your company network
- Use multi-factor authentication (MFA), which is a way of confirming identity using two or more security mechanisms (e.g. username, password and a code sent via text), when available
- If in public, make sure you use a certified public wireless hotspot and be aware of false ones...



9

Always back up important data.

Whether it’s photos or key documents, use an external hard drive or a cloud-based storage system. If your device is infected by a virus, malicious software (malware) or accessed by a cyber-criminal your data may be damaged, deleted or held to ransom by ransomware preventing you from accessing it.



10

Always be cautious of hackers' tricks such as phishing.

Hackers want to trick you into taking an action that grants them access to your device and your organisation's network. Remember to stop, look, and think before taking any sort of action.

- Think twice before sharing information
- Be suspicious of all unexpected messages and social media connection requests
- Cybercriminals are likely to use the current concerns around COVID-19 in phishing attacks. Be cautious of any suspicious or unexpected emails relating to this
- Is this email real or a phishing attack? Phishing emails are disguised to look like they are from familiar contacts or organisations and try to trick you into taking an action like opening a malicious attachment or clicking a malicious link. Always pay close attention to the email domain

At RSA we will only ever email you from a legitimate address, e.g. eu.rsagroup.com, insurancecorporation.com, morethan.com, uk.royalsun.com or uk.rsagroup.com. However be wary that sophisticated cyberattacks can also ‘spoof’ addresses so they appear to be from legitimate domains. Therefore if something doesn’t feel right always check with us through another channel.

Coronavirus related phishing scams are on the rise, but the National Cyber Security Centre have launched a campaign to combat such scammers and help protect you. Over 5,000 suspicious emails have been flagged to the NCSC and 83 malicious web campaigns have been shut down as a consequence of their new email reporting system. It’s now easier than ever to flag any emails you feel are suspicious, by forwarding to report@phishing.gov.uk and they can test the validity of the site.

If you would like to find out more about cyber security, then visit ncsc.gov.uk.