HELPING YOUR COLLEAGUES WORK SECURELY FROM HOME

This guide is to help you understand what to put in place, and what to communicate to your colleagues, to help everyone work from home with security in mind. For many people now working from home, this may be 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, so it is vital at this time to bring the awareness level of employees up as fast as possible. We want you, and your colleagues, to feel confident that you can get on with work safely and securely.

Getting Securely Connected

Ensure that devices are set up securely. In the corporate environment, people rely on their workplace having security structures like firewalls and anti-virus in place, so we need to replicate this at home. Firewalls, anti-virus and automatic updates should all be configured on laptops and mobile devices.

Communicate the need for devices to be kept up to date. If people are using personal devices for working at home, explain why updates are so important. People often don't realise the security implications of updates so explain that, especially at a time like this, we need to make sure our devices are kept as secure as possible, patched from the latest bugs.

Help people understand that they should change the default password on their Wi-Fi router if they haven't already. Provide some guidance on how to do this, explaining why as people may not understand that using a Wi-Fi router that is "protected" by the default password is still risky because default passwords are often easy for cyber criminals to get hold of. Be clear in your communications so that people understand you are not simply talking about the password that people use to connect to the Wi-Fi, but also the password that protects the router itself.

Taking a **risk-based** approach, you may want colleagues to set up 'work', 'home' and 'guest' networks on their Wi-Fi. This way they will segment their home network so that, for example, their children are playing online games on a different network to the one being used for work activity.

Virtual Private Networks (VPNs) come in two different flavours. One is to protect day-to-day internet usage from being attacked, generally when we are connecting to the internet out and about (eg in cafes or hotels). The other type of VPN is a tunnel back into the corporate network, which allows you to extend your office network outside of its physical location. The corporate tunnel solution includes the benefit of protecting your internet connection, bringing it under the corporate network. If you don't already have one of these solutions, it is strongly suggested that you put one in place to protect the organisation and the individuals. Communicate to your colleagues why a VPN is in place and why they should be using it, acknowledging that they may notice a slowdown in the speed of connectivity.

If colleagues are using **personal devices** for work, consider making the services that are available to them over the VPN more restricted than on work devices that are connected via a corporate VPN.

Bandwidth may become an issue for your colleagues so ideally, organisations will make sure that there is a provision to pay for extra bandwidth if people need it. Communicate that this is available for people and set up a process to make it easy for people to request it, and manageable for you to deal with those requests.

Many organisations are going to be holding more conference calls than ever, with people joining from home. There are a few **logistics** to consider here, of course, not least which provider to use. One consideration is to provide people with headsets, which will enable your colleagues to join conference calls online hands-free without the whole call being broadcast for everyone in the vicinity to hear.

Keep Data

In an office environment, it is generally expected that data is automatically backed-up and end-users won't have to think about it. When it comes to home-working, you may require your colleagues to be more active in considering how data is saved and shared.

Set up a secure **file-sharing** system so people can still work together, remotely. You will want to reduce people emailing files to each other and limit the likelihood of people using non-approved file sharing websites. A business decision should be reached as to which file-sharing solution has security in place that your organisation is comfortable with. Again, it is important to communicate this solution to your colleagues in a way that helps them understand why they should be using this approved solution and not emailing documents, which puts a strain on the email system, and not using non-approved file-sharing solutions, which opens up more risk.

As an organisation, **back up** file-sharing solutions if required. Help your colleagues understand how to back up their devices, for example by using Time Machine if they are Mac users. Choose the back-up medium that is right for your organisation, whether utilising the cloud or external hard-drives or a combination of both. Whichever solution you choose, you must encrypt the data whether it is at rest or in transit.

Destroy Data

It is important to encourage your colleagues not to forget about the full life-cycle of data.

Your colleagues may not have a **secure** location to store data, so help them be aware of how important it is that they safeguard data in their possession and securely delete or destroy it when the time comes. For example, if they are using external hard-drives to back up data, issue some advice on where to store the hard-drives and how to secure them. Encourage your colleagues to think about the life-cycle of data and when they should be deleting data that they are creating, storing and backing-up.

Think about your **shredding** solution at home as many of us are used to secure shredding being taken care of for us in the office. Your colleagues may still be printing information at home, but without considering how they dispose of it. Issue guidance that makes your requirements clear. Communicate what information can go in the recycling bin and that if in any doubt, paper should be cross-shredded. Many of your colleagues may not have cross-shredders at home, so you will likely have to provide these for them.

Protecting Credentials

Authentication is always a challenge when it comes to security, but protecting credentials is now more important than ever.

Breaches are a greater risk at a time of crisis, which means that people's credentials are more likely to be compromised. It is more important than ever that we all use unique passwords for each of our accounts; if we are re-using a password and it gets breached, this effectively opens up all of our accounts where the password is being reused.

Password managers enable people to use a complicated and unique password for each of their many accounts. If you don't already have a password manager in place for your colleagues, you may want to consider one now. Some teams may have a business reason for sharing access to accounts, such as social media, and a password manager can support them in sharing passwords securely. If you move ahead with a password manager, communicate why you are rolling this out and issue clear guidance on how to set up and use a password manager (you may want to run online workshops). Ensure you answer the key question people often have about password managers: "don't they put all of my eggs into one basket?". Some thoughts on this, and why using a password manager offers greater security than not using one, can be found at https://www.cygenta.co.uk/guidance

Taking a **layered approach** to protecting accounts is crucial, and this is where two-factor (or multi-factor) authentication (2FA) comes in. As explained above, organisations are at greater risk of being breached during a crisis like COVID-19, which puts people's usernames and passwords at more risk. Having an extra layer of defence on accounts, by setting up 2FA, offers a much greater level of security than simply relying on passwords. As with password managers, when you set up 2FA, communicate why you have done this and help people understand what they need to do and how to do it. There is some information that may help you at https://www.cygenta.co.uk/guidance

Staying Savvy

Unfortunately, cyber criminals take advantage of a crisis. There have already been reports of phishing scams using COVID-19, and this is only likely to increase.

Communicate to your colleagues that social engineering scams are taking advantage of the COVID-19 crisis and that they should be vigilant of any communications that try to entice them into clicking links, downloading documents or giving away information such as usernames or passwords.

Make sure people know that this is **any form** of communication: this includes emails, of course, but also SMS text messages, phone calls, WhatsApp messages, social media messages and more.

Examples of **social engineering** scams can be used in your communications; you will find some information on this at blog.cygenta.co.uk/wfh-guidance/

Help your colleagues **understand** that one of the key red flags of scams is that they play on emotions: they try to get us to feel emotional so that we are not thinking as clearly. Communicate that people should be especially wary of unexpected communications that make them feel emotional, such as scared, panicked, excited, flattered or under time pressure.

Now, more than ever, communicate what people should do if they are involved in an **incident** or receive a phishing message. Help people understand how they should report this and communicate this positively – you don't want people to feel scared about reporting that they may have clicked a link in a phishing email, for example, because this will only drive incidents underground.

You may have to reconsider plans that you have for cyber security **awareness-raising**. Think about how you can use digital methods to communicate awareness messages, for example with webinars and live streams in place of face-to-face workshops and presentations. Don't be afraid to think creatively with this!

The cyber security community is sharing a great deal to help organisations be as secure as possible at this time. Take a look at blog.cygenta.co.uk/wfh-guidance/ for an up to date list of resources and links to other information that may help you.