STAY SAFE IN LOCKDOWN

Security
Backup
Continuity
Compliance

Custodia Continuity

Stay Safe in Lockdown

Table of Contents

Custodia Continuity

Stay Safe in Lockdown

HELLO!

Thank you for downloading this document - we hope it will help you to stay safe and cyber secure while you work from home. We have designed this advice to be simple and cost effective, ideally it will cost you nothing to implement other than a little time and will stop you being the easy low hanging fruit for the cyber criminal.

This advice will not stop everything, but it will help to keep you safe from casual attacks and now you have all your sensitive data at home it is important to take the time to secure yourself.

If you have any concerns about your security, give us a call, , and one of our amazing team will be on hand to help.

Custodia Continuity
01629 369250
help@custodiauk.com
www.custodiauk.com

If you would like to write to us, then it's:

Custodia Continuity
The Old Blacksmiths
The Dale
Wirksworth
Derbyshire DE4 4EJ

We are here to help - we don't do hard-selling, we don't apply pressure or create fear.
We love answering questions and we love to meet new people and help solve problems.

We look forward to hearing from you.

Chris and Jae – Directors; Custodia Continuity

Stay safe out there

Systems and Hardware

It is important to make sure your hardware is protected, at work you may have an IT department who help secure your equipment, at home this may be overlooked. This is especially important for your router, to make sure the bad guys stay on the outside of your home network.

Make sure you have virus protection on all your computers. It's great having your work laptop secured but a virus on the old laptop that the kids use will soon find it's way to the rest of the network. Windows defender is great and comes free with your windows pc. It can be accessed from settings in the start menu.

Is your router firewall turned on? Have a look at the management page on your router (connection details are usually on the back of your router.) and make sure your network is secured. If in doubt, call your internet provider.

Are your disks encrypted? There are links at the end of the document to articles that can help you to do this on both Windows and Apple computers. Encryption stops a person who may have taken your hardware from accessing any data.

Are you using personal IT devices for work? If so you need to be especially careful. Make sure you take care online and if you aren't sure we suggest that you get a temporary device for work if possible.

Software and Patches

If you are using remote meeting software is it secured? Have you ensured that all your meetings are password protected?
We suggest that you also turn off file sharing in virtual meetings to ensure that malicious data can't be easily shared.

This is especially important if you also use social media during lockdown on the same computer.

Are you happy and confident with any remote access software you have to use?
If not, can you easily get advice support and training?
It is very easy to accidentally delete data that isn't recoverable if you are not confident with the software you are using.

A software patch is an update released by the software developer to improve the service their application provides and more importantly to often close a hole in the applications security.

Most software patches are automatic, the annoying pop ups that tell you to close all windows so the software can update.

Its irritating but crucially important. Software patches contain security fixes to keep you safe. Make sure yours are up to date, click "yes update now" and have a coffee break. Links at the end of this document show you how to ensure updates are applied to your computer automatically.

Custodia Continuity

Stay Safe in Lockdown

Networks & WIFI

We suggest that you split your wireless network at home into personal (for the kids and Netflix) and a work network just for you with separate passwords.
This can help keep you safe if the kids accidentally download something nasty, plus you can put your printer on this second work network to avoid having all the paper in your office turned into easy-colour Peppa Pig scenes.

Most home routers will allow you to do this, check out the online users guide from your provider or give them a call. If they can't help, give us a call!

Do you change WIFI passwords regularly?

Now we are all taking our work home we cannot stress the importance of this enough.
Change the password so that your traffic stays absolutely secure.
Who knows who the kids have given the password to.
Another great reason to create a second work network.

Have you changed your routers default access login details?
The default login details are available for most routers with a quick internet search.
Hackers will try default passwords and logins on most common routers.
We cannot stress this enough, change the default login information.
Details of how to access the control panel to change this are often on the back of your router. If You aren't sure contact your internet provider or give us a call and we will help.

Custodia Continuity

Stay Safe in Lockdown

Backup of critical data

Backup is the best way to ensure you don't lose data. It will help protect you from ransomware and malware infections as well as ensuring you don't accidentally and permanently delete anything important.

Do you backup all your essential data at least once a day?
Get an external hard drive or an online backup and get that data secured.
Apple time machine is very good and there are several windows solutions that are automatic and cheap.
Don't delay, backup today!

Are you using cloud services?
Cloud services guarantee the service not the data in the service. Make sure you have backed up all your essential data especially if it is stored in the cloud.

Do you have a clear recovery plan, should you have a data breach or ransomware attack?

Make a plan so should you lose some or all your data you are ready to deal with the loss.
How will you inform customers?
What data is recoverable?
How will the business continue?
All important questions to answer before a data breach.

Custodia Continuity

Stay Safe in Lockdown

Mobile Devices

We all use them, and they are often the weak security link in the chain.

Do you use social media on your mobile?
Do you also use the same device for work?

Be very cautious. Painfully, savagely cautious, particularly if you are an Android user.

There are some nasty things out there on social media at the moment and it is a huge security risk
.
Mobiles are generally less secure than home computers just because they can be more easily lost, we take data out and about on them everywhere we go and are they used for a wide range of activities both social and work related.

We would suggest getting a temporary device just for work.

If possible, buy a super cheap work phone (you can pick up a simple smart phone for £30 or so and a sim only contract is under £10 a month with some providers) and keep personal and work separate and therefore safer.

Attachments on WhatsApp are particularly unsafe at the moment.
A common threat at the moment is activated by opening an attachment in a message from a trusted source, friend, grand-parent etc whose account has been hacked.

The attachment to the message will infect your device, copy your keystrokes to a remote hacker thus giving them all your logins and passwords. Bad times.

Custodia Continuity

Stay Safe in Lockdown

PASSWORDS

You have heard this before, we know, but it is crucially important, now more than ever.

Change you passwords, make them hard to guess, but easy to remember, (GreatCoalSandwich!! would be a great password, hard to guess, easy to remember) use a password manager (there are lots out there, LastPass or 1Password are the front runners) that are cheap, integrate with your browser and apps and will help keep you safe.

PHISHING

There really isn't much I can say. If an offer is too good to be true it won't be true.

Check the sender, if you click on the sender line in the email it will show the actual address the email is from not the spoofed address.

If you are in any way not sure give the sender a call if you can. Or check online to see if the World Health Organisation really are offering $50000 dollars for vaccination testers.

Seriously though this is the most common attack that succeeds by playing on our fears.

Do not open links in emails if you are not certain they are ok. If in doubt call the sender.

Do not download files from email attachments unless you are likewise sure. If in doubt call the sender.

Custodia Continuity

Stay Safe in Lockdown

Banks, the HMRC, Amazon, the NHS will never ever ever under any circumstances ask for password details or your bank details.

Microsoft will not call you up and ask to help you with your computer.

If anyone ever asks you to install software on your computer no matter how legitimate it sounds, don't do it until you are absolutely certain it is ok.

Be Aware
Be suspicious
Be safe

We hope this guide has been useful, share it if you think it could help someone.

Stay safe in these times of change and if you are worried at all give us a call and our reassuring and helpful team will always be here to help guide you.

Remember, if you have an IT department, always check with them before following anyone's advice!

Links:

Encrypting Windows computers:
http://bitly.ws/89A4

Encrypting Mac computers:
http://bitly.ws/89A5

Updating Windows 10:
http://bitly.ws/89A9

Keeping a mac up to date:
http://bitly.ws/89Ab

Custodia Continuity

Stay Safe in Lockdown

About Us

We are a small Cyber Security company based in Lincoln who believe that security shouldn't be a DIY experience and that top-class cyber security should be affordable for all.
We turn cyber security, backup, business continuity and regulatory compliance into a simple service with a personal relationship for everyone.

Our security work is based on four core pillars that are the corner stones of good security

1. Best in class Network security solutions that keep the bad stuff on the outside of all your networks

2. An ultra-secure backup solution that is off cloud and offline, to protect clients against ransomware attacks.

3. Disaster recovery testing and continuity planning, we work with our clients not only to create their planning but to be there if they need to execute it as well.

4. And our final core product is a complete and continuously maintained Regulatory Policy pack, from GDPR, DPA2018 to IT Security policy and modern slavery.

We level the playing field for small and medium enterprises and let them compete with the big corporates when it comes to demonstrating competence and compliance with data and security.

We know that a business's security is as bespoke as its product and service so every solution we design is tailored with the customer in mind and is always responsive as the customers business's needs change.

No hard sell, no fear mongering just a good old fashioned and responsive relationship to keep you and your customers safe.
No dashboards, no support tickets no do it yourself solutions, just good personal service 365 days a year 24 hours a day.