exponential-e
APPLIED INNOVATION

USER GUIDE
UNIFIED COMMUNICATIONS

Working From Home Checklist

Implications of working from home due to COVID-19

Due to Government instruction, the majority of UK employees are now working from home, in an effort to minimise the drastic effects of COVID-19. Some employees already have already worked remotely in the past, but for many, this will be a new experience. With a combination of remote workers and a potentially depleted workforce, there is an increased likelihood of a cyberattack or data breach occurring. Cyberattacks have already gone up 37% in the past month, as the COVID-19 pandemic provides cyber-criminals with new ways to exploit both individuals and corporate infrastructure. With most technical teams and staff working from home, there has never been a worse time to suffer a cyber-incident.

That's why Exponential-e have created this document, to clarify why security is important in these difficult times, and demonstrate best practice to support your technical teams, avoiding any potential security incidents or exploitable vulnerabilities.

01. Educate Yourself

As a user, you play a vital role in your business' overall cyber-security strategy. Without vital education and awareness, even businesses with the most robust cyber-security eco-systems will inevitably fail. So, what can you do to make sure you are well-equipped and reduce any risks to your network?

Regular training

Attend as many webinars and training exercises as possible. These should help make clear the importance of your role in securing the business. Ensure you learn about best practices – both in the workplace and more importantly at home working remotely – so you can improve your own security practices.

Know your business' security systems

Make sure you know exactly how to access the company network and data in a safe and secure manner. If you have any doubts, consult your IT team or a technical colleague, rather than the internet. Your IT team has created a secure solution for remote working, so please do not move data to other solutions or try to bypass them, as this will lead to vulnerabilities and – in turn – security incidents.

Exponential-e Ltd
100 Leman Street, London
E1 8EU

Telephone
+44 (0) 845 470 4001

Visit the website
www.exponential-e.com

Email
info@exponential-e.com

Follow us on Twitter
@exponential_e

02. Use Strong Passwords

There are a few key rules when it comes to passwords, to ensure cyber-criminals cannot access your data:

Do not re-use passwords

In this day and age, the average user has over 30 passwords to remember, making it hard to keep track of them – but please do not use the same one repeatedly. Using a different password for every account or online profile is vital in stopping even the least sophisticated hackers from attempting to use that username and password combination on the most popular websites, including Facebook, Twitter and Amazon. Doing so will protect you from fraud, identity theft, and reputational damage.

Create strong passwords

Whilst we have been told for years that strong passwords are made of letters, numbers and symbols, with a minimum of 8 characters, the truth is less complicated. At a minimum, you'll need a 14-character password.

The NCSC recommends using three random words strung together. Length is the primary factor when creating a strong password; the longer it is, the more guesses it will take to get it right.

Exponential-e would recommend...

Using a password manager (e.g. Dashline or Lastpass, which are free!), to generate different, random passwords for every login portal. Password managers securely store all your passwords and automate logins to every system. At the end of the day though, the best solution is to always use 2FA or MFA.

03. 2FA or MFA

Two-Factor Authentication (2FA) and Multi-Factor Authentication (MFA) are secondary layers of security. Whenever you input the correct username and password, you will need a secondary code, delivered by email, text message or hardware token. This ensures the person logging in is the correct one.

There are plenty of 2FA solutions available, which your IT team will be happy to set up for you.

It is important to note that:

- Identity theft is an easy, low-risk, high-reward type of crime, and a threat to all businesses. It is the fastest-growing type of crime and is now more profitable than drug-related crimes.
- Weak or stolen user credentials are most hackers' weapon of choice, used in 95% of all web application attacks.
- From 2013-14, the number of successful data breaches went up by 27.5%.
- Household-name companies are often the victims of cyberattacks, however, they are not the only ones being targeted. Of all targeted attacks, 31% are aimed at businesses with less than 250 employees.
- Anti-virus systems and advanced firewalls are necessary security elements, as are vulnerability tests. But even with all these security measures in place, without user authentication, the front door is still wide open to intruders.
- Password theft is constantly evolving, as hackers employ methods like keylogging, phishing, and pharming.
- Cyber criminals do more than simply steal data. They also regularly damage data, change programs or services, or use servers to transmit propaganda, spam, or malicious code.

Exponential-e Ltd
100 Leman Street, London
E1 8EU

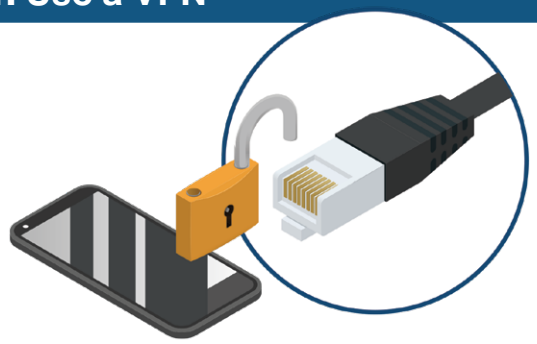
Telephone
+44 (0) 845 470 4001

Visit the website
www.exponential-e.com

Email
info@exponential-e.com

Follow us on Twitter
@exponential_e

04. Use a VPN



Experienced remote workers will already be familiar with using a Virtual Private Network (VPN) to connect to their organisation's infrastructure, but for most office workers, this is a brand-new process that they will need to take the time to understand and become accustomed to.

A VPN is critically important in securing data as it moves across the internet. A VPN will encrypt all of your internet traffic, so that it is unreadable to anyone who might be trying to intercept it. This keeps it secure from the prying eyes of any eavesdroppers; including cyber-criminals and hackers.

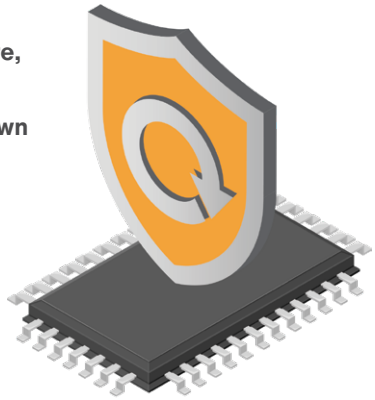
The use of a VPN might slow down internet speeds, but it will ensure that only authorised individuals can see your data. If you need to perform high-bandwidth tasks – such as holding video conference calls – you might need to use a cloud-based solution, but your IT team will be able to advise you in this regard.

05. Regularly Install Updates

Updates to applications, operating systems and hardware can be an extreme source of annoyance to most individuals. But they are vitally important, as the updates provided by manufactures and software providers, often include patches for security vulnerabilities. These vulnerabilities will have been uncovered by cyber-criminals and/or developers and could be exploited to gain access to sensitive data or infrastructure.

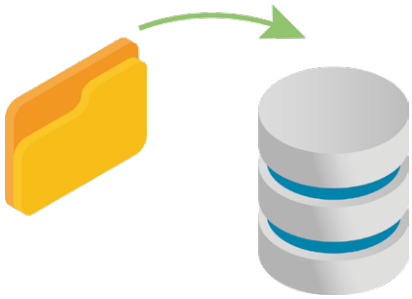
Most systems are designed to install updates automatically, but some individuals turn off automatic updates, often due to a bad experience with faulty patches. Nonetheless, it is more vital than ever to enable patching and ensure systems are properly protected.

If infected with malware, just one vulnerable system could bring down a global organisation.



06. Backup your Data

Having duplicate copies of your most important information saved in a remote location ensures it is safe, in case anything goes severely wrong with any of your computers or servers.



Thankfully, for those who have adopted a cloud-based strategy, back-up is usually automated and disaster recovery is built-in. However, for those who store their data in on-premise solutions, it is necessary to make sure that they have an automated back-up to cloud or off-premises storage, in case of breaches, hardware failures, fire or theft scenarios.

Remember, for back-ups to work, whatever it is backing up must be connected to the internet.

Use external, encrypted hard drives in cloud solutions where possible, even if your business hasn't yet adopted a cloud-based strategy.

Exponential-e Ltd
100 Leman Street, London
E1 8EU

Telephone
+44 (0) 845 470 4001

Visit the website
www.exponential-e.com

Email
info@exponential-e.com

Follow us on Twitter
@exponential_e

07. Look out for Phishing Emails and Spoofed Websites

Phishing attempts have increased by over 600% since the end of February, with traditional vectors including impersonation scams, but also newer, business email compromises and extortion attacks.

Attackers will attempt to trick you, using phishing, vishing, whaling, and many other malicious techniques, so it is important that you are vigilant and double check every email. Use your common sense to protect yourself and your organisation.

Tips for email security:

- Double check who the email has been received from and make sure their email address is correct
- Hold your mouse over any link to see the full URL. Suspicious links are probably unsafe, so report any to the IT team or personally delete the emails
- If you are unsure, find the website manually, by typing the address into your browser to open the page, instead of using the potentially malicious link
- Avoid clicking on any attachments from untrustworthy individuals or emails you were not expecting. Always double check and contact the sender first!

Try using alternative ways of contacting the apparent sender, outside of the suspicious email chain. The safest methods of verifying a potentially malicious email are through text messages or online messaging.

After all, the cyber-criminals do not have access to everything at once!

08. Use Antivirus Software

Always use a trusted antivirus (AV) software, as many of today's antivirus companies are seeing 400,000+ versions of different malware per day. AV can act as the next line of defence, by detecting and blocking known malware. Consider the unknown malware as well, known as 'Zero Day' or 'Signature Less', and use next-generation protection to enhance the line of defence.

If you're not already using one, Exponential-e recommends best-of-breed solutions, such as Custodian 360 and Sophos, which are able to provide invaluable protection.

Even if malware manages to find its way onto your device, an antivirus solution may be able to detect it, and in some cases, remove it. Be vigilant, and if your system starts to act differently, please contact your IT team to ensure there is no infection.

09. Secure your Home Router

Your home wireless router requires a password, to allow you to connect your computers, mobile devices and smart devices over Wi-Fi. Routers frequently come with a pre-set password, which is common to all other routers provided by your ISP. If this is the case, you should change this password immediately, ensuring your router remains secure. Alternatively, you may choose to change your router password to make it easier to remember, especially when visitors to your home or office want to connect.

Your router also has an SSID (Service Set Identifier), which is the Wi-Fi name that appears in searches for local networks. Again, this is often the same as all other SSIDs from the same manufacturer, which does not only cause confusion when searching for a network, but also highlights to hackers, that your router security 'hygiene' is lax.

There are a number of helpful guides online to help you with this.

Exponential-e Ltd
100 Leman Street, London
E1 8EU

Telephone
+44 (0) 845 470 4001

Visit the website
www.exponential-e.com

Email
info@exponential-e.com

Follow us on Twitter
@exponential_e

10. Exercise Caution with Remote Desktop Tools

Your business's IT team will generally use one specific remote desktop tool to allow you to raise an issue via your device, i.e. TeamViewer or Microsoft Remote Desktop. Make sure you know which tool this is.

If you see any of the following happen, remove your device from the network and contact your IT administrator immediately, as it could be malicious:

- A pop-up for an unknown RDP that isn't used by your company
- Someone requesting access to your device, without you requesting assistance from IT Support
- Loss of control of your device, where you are only able to view activity occurring

11. Watch out for 'Work from Home' Scams

In our current cyber landscape, it is important to be aware of some of all the most recent scams. In the last few weeks, over 60,000+ websites have been created around COVID-19, with 302 fake websites selling 'home-testing kits' and 44 sites apparently selling a cure.

These must be avoided at all costs, as they will take money from the deceived individual or infect their machine with malware.

12. Use Encrypted Communications

When sending your next email think, "Should this be encrypted?", as personal information and other forms of sensitive information must be protected during communication.

Many companies now have methods for sharing documents outside of email, ensuring they are appropriately secured. Your IT team will be able to advise you if you are unsure of the best way to share sensitive documents, in order to keep them safe from hackers.

13. Lock your Device

How many times have you seen someone leave their device open for anyone to access in a public place? Fortunately, with the current lockdown, this is less of an issue. However, please remember a family member could still send the wrong messages to the wrong people or access an unsecure website.

It is therefore important to keep your device and your business' data secure. Lock your device with its password, because if data is leaked, fines could be costly.

Where possible, use device encryption on your laptop's hard drive.

We hope this checklist proves useful during these unprecedented times. If you need any further guidance or support, please do not hesitate to contact your IT team or Exponential-e.

In the meantime, stay safe!

Exponential-e

Telephone
+44 (0) 845 470 4001

Visit the website
www.exponential-e.com