Data Sheet

DTS SOLUTION
CYBER SECURITY REDEFINED

Work From Home (WFH)
Cyber Security Plan

While the current COVID 19 outbreak has put the pressure on economies this is a stressful time given the uncertainties, it's also a great time for seeing how ready your organization is for emergencies and other remote worker needs. Even if you don't tell everyone to work from home, take the time to think about if you could make everyone work from home and how well you could do it.

Document WFH Policy & Procedures

- A written policy should be in place that governs remote workers with clear & uniform rules.
- Focus on the job responsibilities, organizational, departmental goals & objectives, customer impact & employee's work performance.
- Be aware & manage your risks.

Have a Security Game Plan

- Remote workers need the same access to applications, tools & peers as they do when in office environment.
- Reinforce your policies & practices regarding protection of customer sensitive data. This is especially important is employees with customer facing & customer support roles who may have access to sensitive & critical information.

Monitor & Manage

- Automate security where possible.
- Updates of end point device software and other applications can be a source of annoyance, but they really are important. Updates often include patches for security vulnerabilities that have been uncovered since the last version of the software was released.
- Protecting customer sensitive data is first priority. Support this by enabling software updates in to the applications your remote workers use without requiring any human intervention.
- Communicate & educate: keep security awareness training and mentoring WFH workers.

Use Strong Passwords

- Unfortunately, many people still use the same password across multiple accounts. This means that all it takes is one compromised password for a hacker to take over all of your accounts.
- It's as important as ever to ensure that all accounts are protected with strong passwords.
- Passwords should be unique for every account and should comprise a long string of upper and lower case letters, numbers, and special characters.
- It's difficult to remember all these passwords, which is why password managers are such popular tools these days.

Multi-factor Authentication - 2FA

- Having a strong password often isn't enough, for example, if your credentials are leaked in a data breach. Two -factor authentication (2FA) and two-step verification (2SV) involve an additional step to add an extra layer of protection to your accounts.
- The extra step could be an email or text message (OTP) confirmation, a biometric method such as facial recognition or a fingerprint scan, or something physical, such as a USB fob.

Work From Home (WFH) Cyber Security Plan

Use Virtual Private Network (VPN) Connectivity

- Certain applications require Virtual Private Network (VPN) connectivity (i.e. VoIP. Provide employees with easy to use documentation & job aides regarding how to log in remote network services such as VPN, telephone service, etc…, including password procedures.
- VPN has another important role, and that's improving your online privacy. A VPN encrypts all of your internet traffic, so that it is unreadable to anyone who intercepts it. This keeps it away from the prying eyes of any snoopers, including your Internet Service Provider (ISP), government agencies, or hackers.

Use Advanced Endpoint Detection and Response

- Deploy EDR technology also known as NGAV on your endpoints. When your systems are not inside your corporate network the risk factors multiply and for that you need comprehensive endpoint security suite.

Secure the Home Router

- Have you changed you home router password recently?
- Many people do not, leaving their home network vulnerable. It's important to take simple steps to protect your home network to prevent malicious parties having access to connected devices.
- The encryption should be set to WPA2 or WPA3. Restrict inbound and outbound traffic, use the highest level of encryption available, and switch off WPS.

Firewall Setup

- Firewalls act as a line defense to prevent threats entering your system, they create a barrier between your device and the internet by closing ports to communication. This can help prevent malicious programs entering and can stop data leaking from your device.
- Your device's operating system will typically have a built-in firewall. In addition hardware firewalls are built in to many routers. Just make sure that yours are enabled.

Perform Backups

- Data can be lost in a number of ways, including human error, physical damage to hardware, or a cyber-attack. Ransomware and other types of malware can wipe entire systems without you having a chance to spot it.

Be on the Lookout for Phishing – Be the Human Firewall

- To spot a phishing email, check the sender's email address for spelling errors and look for poor grammar in the subject line and email body. Hover over links to see the URL and don't click links or attachments unless you trust the sender 100 percent. If in any doubt, contact the alleged sender using a phone number or email address that you find somewhere other than in the suspicious email.
- If you do click & end up on a legitimate-looking site, be sure to check its credibility before entering any information. Common signs of a phishing site include lack of an HTTPS padlock symbol (although phishing sites increasingly have SSL certificates), misspelled domain names, poor spelling and grammar, lack of an "about" page, and missing contact information.

Be on the Lookout for WFH Scams (COVID-19 Scams)

- As well as targeted phishing attacks, we're likely to see an increase in work-from-home scams. Many of these request personal information or upfront payments before you can begin work. By the time you realize it's a scam, the fraudster has ceased contact and stolen your money or taken over accounts.
- Never share personal information with a client that you haven't thoroughly researched. And don't work with anyone who requests an upfront fee.
- Also be on the lookout for pyramid and multi-level-marketing (MLM) scams as these are often well-disguised as legitimate and attractive work-from-home opportunities.

Take Advantage of Your Cloud Storage

- Most organizations have access to huge cloud storage (Google/AWS/Azure), put that online storage to good use & encourage your workers to keep everything stored on the cloud to make collaboration easier.

Don't Be Afraid to Use Cloud Services

- Cloud based solutions can solve business challenges quickly & scale when used correctly.
- Enable your employees to trial solutions for their specific problem sets & support them if and when they need to roll them out more widely.

DTS SOLUTION
CYBER SECURITY REDEFINED

DUBAI: Office 4, Oasis Center, Sheikh Zayed Road, Dubai, United Arab Emirates
T: +971 4 338 3365 | **E:** info@dts-solution.com

800 HACKED

ABU DHABI: Office 253, Al Bateen C6 Tower - Bainunah, King Abdullah Bin Abdulaziz Al Saud Street | **T:** 971 2 2076777
LONDON: 160 Kemp House, City Road, London, EC1V 2NX, United Kingdom | **T:** +44 2081230 387 (DTS)
www.dts-solution.com