MARSH

Security Tips for Remote Working

Protecting Your Business during a Pandemic

Corporate IT Security

- Provide employees with regular communication and awareness messages, including basic security knowledge:
  - Beware of phishing, especially COVID-19 scams and fraudulent COVID-19 websites
  - Know working from home "DOs & DON'Ts"
  - Ensure home Wi-Fi is secure
  - Always use VPN on public Wi-Fi
  - Etc.
- Create a shared channel called #phishing-attacks or an email address to forward suspicious emails
- Update your company's Acceptable Use Policy to address working from home and the use of home computer assets
- Identify functions that can only be undertaken in a secured environment at the office (i.e. not remotely)
- Develop COVID-19 specific playbooks and adapt disaster recovery plans to current context
- Provision protective technology on endpoints (hardening, anti-virus, endpoint detection and response, etc.)
- Enforce software updates
- Utilize a password manager or run password audits
- Tighten and test access control procedures, especially for change in workforce and internal threats
- Provision for the load of increased number of remote users
- Provide VPN access and disable split tunneling
- Enable multi-factor authentication everywhere, especially on email accounts
- Re-assess rules, like geo-blocking and similar ones, that could prevent remote access
- Ensure continuity of access when IP whitelisting is in use
- Use MDM/EMM solutions and enforce mandatory remote backups on select users or repositories
- Provide home security checks for employees through phone technical support

Home Security (for employees)

- Reset default home Wi-Fi router passwords and enable WPA2 encryption
- Never leave your laptop and other mobile devices unattended in public space or unlocked at home
- Keep your work separate – don't use work laptop for personal matters, let family members use it, or use personal laptop for work
- Avoid the use of USB sticks and other removable storage
- Use company pre-approved cloud or data center storage instead of local or personal storage
- While working from home, mute or shut down any digital assistants (e.g., Alexa, Google Home, etc.) since they are constantly recording nearby conversations
- Maintain a clean work area and enable a 5 minute screen lock
- Store any paper documents securely and dispose of by using a shredder
- When necessary, save VPN bandwidth for your organization:
  - Use VPN only for sensitive communications, not for internet browsing or personal matters
  - Limit use of videoconferencing, and use audio through phone instead of computer

Consider these recommendations within the specific context of your organization's operations and IT infrastructure. For more information on how Marsh can help the cyber needs of your company, contact your Marsh representative or reach out directly to:

TALAL Y. DARRAS
Business and Cyber Resilience Leader - MENA
Marsh Risk Consulting
+971 56 174 0379
talal.darras@marsh.com

SIMON BELL
Financial and Professional Lines Leader - MENA
+971 50 450 1935
simon.bell@marsh.com

PEPIJN DE JONG
Cyber Resilience Practice Leader - MENA
+971 50 489 0486
pepijn.de-jong@marsh.com