



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
- Utilise 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:

marketingafrica@marsh.com

Marsh (Botswana) (Pty) Ltd is one of the Marsh & McLennan Companies, together with Guy Carpenter, Mercer, and Oliver Wyman. This document is not intended to be taken as advice regarding any individual situation and should not be relied upon as such. The information contained herein is based on sources we believe reliable, but we make no representation or warranty as to its accuracy. Marsh (Botswana) (Pty) Ltd shall have no obligation to update this publication and shall have no liability to you or any other party arising out of this publication or any matter contained herein. Any statements concerning actuarial, tax, accounting, or legal matters are based solely on our experience as insurance brokers and risk consultants and are not to be relied upon as actuarial, accounting, tax, or legal advice, for which you should consult your own professional advisors. Any modeling, analytics, or projections are subject to inherent uncertainty, and the Marsh Analysis could be materially affected if any underlying assumptions, conditions, information, or factors are inaccurate or incomplete or should change. Marsh (Botswana) (Pty) Ltd makes no representation or warranty concerning the application of policy wordings or the financial condition or solvency of insurers or re-insurers.

Marsh (Botswana) (Pty) Ltd makes no assurances regarding the availability, cost, or terms of insurance coverage. Marsh (Botswana) (Pty) Ltd is regulated by NBFIRA (Non-Bank Financial Institutions Regulatory Authority) License number: 2/9/31 The content of this document is subject to copyright protection. Reproduction of the content, or any part of it, other than for non-commercial educational or personal use only is prohibited without prior written consent from Marsh (Botswana) (Pty) Ltd.

Copyright © 2020 Marsh (Botswana) (Pty) Ltd. All rights reserved.