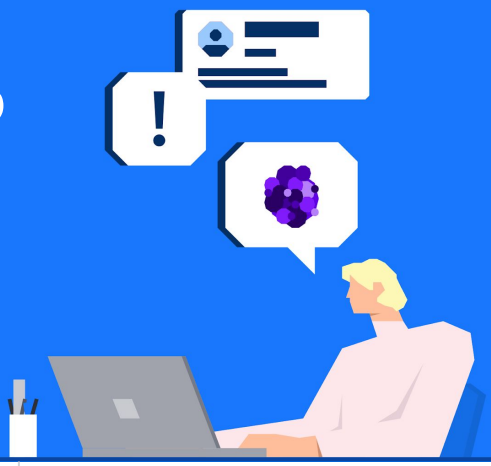
Checklist: How to Stay Secure While Working Remotely



FOR BUSINESSES

- [ ] Keep security policy points and procedures clear and concise
- [ ] Consider how you can enable remote technical support functions
- [ ] Ensure your support team is trained and briefed to offer reassurance and understanding when a security issue arises
- [ ] Always communicate the implementation of new tools or software, including guidelines on how to use them
- [ ] Require remote workers to us VPN for work-related tasks
- [ ] Require every employee use MFA
- [ ] Monitor when new forwarding rules are created; in some cases, disable auto-forwarding rules all together

FOR EMPLOYEES

- [ ] Use company-approved cloud or VPN services instead of emailing sensitive information to your personal email accounts
- [ ] Don't download new software or tools without consulting your IT team
- [ ] Keep your software and operating systems up-to-date
- [ ] Avoid public Wi-Fi and don't rely on personal hotspots
- [ ] If you have mailbox forwarding in place, double check it to ensure it hasn't been compromised
- [ ] If you make a mistake that could compromise security, notify your IT team ASAP
- [ ] Report near-misses, too! This feedback raises awareness and makes everyone safer