MARSH

12 Cybersecurity Tips For Your Home Office

TIP #1

Allow

remote access through a secure channel (e.g. VPN)

TIP #2

Secure

access through two-factor authentication

TIP #3

Use

remote services only via secure protocols (HTTPS)

TIP #4

Limit

remote access just to approved services and isolated areas on the network

TIP #5

Authenticate

controls on remote computers (e.g. antivirus, updates, security settings, etc.)

TIP #6

Authenticate

remote erase and lock capabilities
on computers

TIP #7

Ensure

that personal computers have Full Disk Encryption (FDE)

TIP #8

BACKUP

critical information

TIP #9

Awareness, Awareness, Awareness!

(e.g. how to detect phishing, malicious emails, etc.)

TIP #10

Define

protocols for users to report any anomalous or suspicious situations

TIP #11

Increase

monitoring levels of security events

Some examples:

- Failed and then successful authentication attempts
- Access with the same user from multiple IP addresses
- Suspicious network traffic
- Connections from anomalous locations
  (e.g. unusual countries)

MARSH

TIP #12

Recommend

against the use of public or insecure network connections

MARSH

Applying these simple tips could make all the difference

For more information visit www.marsh.com or contact:

Jean Bayon de La Tour
Head of Cyber – Continental Europe
+49 152 0162 6445
Jean.bayondelatour@marsh.com