CORONA VIRUS (COVID -19)

SECURITY ADVISORY TO WORK FROM HOME

THE IMPACT OF CORONA ON CURRENT BUSINESS LANDSCAPE

All of us know how the threat of Corona (the biological virus) has been growing and sending different cities & countries in the world into a shutdown.

Businesses amidst the spreading of coronavirus under government and social obligations require employing distancing techniques and are asking employees to work from home.

We have also taken a step in the same direction, but we would like to make you aware on some of the best practices in the cyber world while you operate from home.

RISE OF CYBER ATTACKS

IT Experts should keep a number of things in mind, before initiating work from home to ensure preparedness from IT Security perspective.

Have we enforced controls to manage and control only business critical applications to run on end points under WFH mode?

How do we ensure sensitive data is controlled in end points when user is working from home using unprotected Wi-Fi or Hotspots?

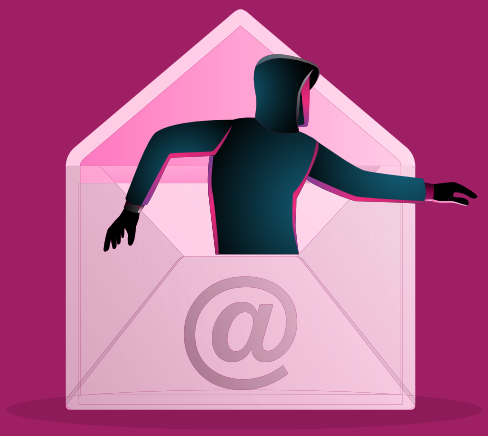
Are we able to monitor and manage employee active time on business vs non business during work from home mode?

Are we able to comply with data leak requirements as enforced by regulator or enforced under client contracts that is required for remote users?

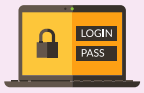
APT36 TAPS CORONAVIRUS AS 'GOLDEN OPPORTUNITY' TO SPREAD CRIMSON RAT

IN CYBER SECURITY CIRCLES, THE CORONAVIRUS IS SPURRING ANXIETY OVER THE VIRTUAL ABUSE OF THE DEADLY DISEASE BY SCAMMERS

CYBER CRIMINALS USING CORONAVIRUS TO CARRY OUT PHISHING ATTACK



'Phishing' emails might appear to be from WHO, and will ask users to:



Give sensitive information, such as usernames or passwords

Click a malicious link

Open a malicious attachment

BELOW TIPS CAN HELP YOU IDENTIFY A PHISHING ATTACK

1. Verify the sender by checking their email address
2. Check the link before you click
3. Be careful when providing personal information
4. Do not rush or feel under pressure
5. If you gave sensitive information, don't panic
6. If you see a scam, report it to your Infosec team

BE CAUTIOUS OF

Using Public Wi-Fi: Public Wi-Fi can be vulnerable to malicious attack, presenting issues for those employees who may need to work from home. We suggest avoid connecting to Public Wi-Fi, they can be vulnerable not only to you, but to the whole organization.

Using Public Computers: Employees should be aware of the security implications of this and adhere to the following guidance: keep screens private (position them away from other people), don't use public computers for any sensitive information, use 'private browsing' where possible, never use 'remember me' or 'save information', and clear your browsing history and delete any downloads before closing the browser.

Accidental Risks at Home: Even when your employees are working from home using your secure VPN, VDI or remote desktop, there can be other risks that need to be considered. Children and pets can be a surprising threat.

Device Security: While your IT team will ensure to update your systems with basic set of security features including latest Anti-virus, Data leakage prevention, encryption etc. It is your responsibility to ensure nothing in the list turns red and follow basic security hygiene.

RECOMMENDATIONS

Save Save Save: To avoid frustration of re-working, make sure you save your work before you step away from laptop; keep your charger handy.

Use a Secure Connection: You must secure your Wi-Fi connections by configuring encryption (WPA2) and enforcing a username and password for connection; Your passwords shall be of two types - One is Router Password; Second is WIFI Network Password.

Use Personal Hotspot instead of Public Wi-Fi: Avoid connecting to Public Wi-Fi and use personal hotspot to have a secure connection.

Password Hygiene: Strong passwords will not only protect your devices and systems being accessed if a mobile or laptop is lost or stolen, they also protect businesses from hackers; always use at least 8 character password with a combination of alphabets, numbers and special characters (*,%,#,@,$,^).

Beware of Suspicious Emails: Beware of phishing emails, double check before you open an attachment. If it is a suspicious email, do not open. Seek advice from IT Helpdesk or Security team. Same applies to SMS's & Phone calls as well.

Beware of downloading official data on personal computers: While you may be required to work from home, we do not encourage use of personal computers for official work, hence do not download any official data on your personal computers.

PRUDENT
THE FUTURE OF INSURANCE

STAY HEALTHY, STAY CALM

We wish you and your family good health during this precarious time. We are confident that this too shall pass and we look forward to seeing everyone together in the office soon.

If you have any questions regarding Cyber Insurance, please write to

neha.anand@prudentbrokers.com

PRUDENT INSURANCE BROKERS PVT. LTD.

Registered Office 101, Tower B, Peninsula Business Park, G.K. Marg, Lower Parel, Mumbai - 400 013, Maharashtra, Tel: +91 22 3306 6000

CIN No.: U70100MH1982PTC027681 | License No. 291 (18th February 2020 to 17th February 2023)

Insurance is the subject matter of solicitation.

Advt2020May002