WHITEPAPER **2020**

Remote Employee Security Playbook

www.**trustifi**.com

Trustifi

Amid the global health crisis the CDC has enacted travel bans and it is now becoming commonplace for organizations to make **their staff telecommute and work from home.**

Home-based workers are often vulnerable to malicious attacks on their networks, and current media reports have suggested that hackers may attempt to take advantage of the surge in telecommuters by targeting remote networks.

*Removing workers from security controlled environments like the office and enabling them to work from home with less security protocols, firewalls, VPN's and oversight, **you are putting your company and its data at risk**.*

Email data is often the most common entry point for these attacks. Companies including Facebook, Amazon, LinkedIn, Microsoft, and Google have asked at least a portion of their employees to work from home in reaction to the current crisis, now being called a pandemic.

Don't panic...plan.

It is important for your organization to maintain a secure work environment regardless of where you and your employees are located. The below precautions were developed by Trustifi's *Information Security and Compliance Officer* & *Chief Technical Officer* to offer assistance to organizations globally to prevent security breaches and attacks.

General Safeguards

- **Keep passwords strong** and varied and use a password manager that also creates strong passwords for you – try to avoid using the same password for many services
- **Do not use free Wi-Fi** - use only one that you can trust
- **Rely on Two-Factor Authentication to login** to all your web services - Passwords can often be compromised or stolen, but with 2FA, the chances of someone also has the additional security question's answer or a PIN is unlikely
- Turn on your **firewall**
- **Encrypt** your disk
- Enable **encrypted backups**
- Use **SSH keys**
- Use a **secure internet** connection

Email Related Precautions

Avoid opening emails and attachments **from unknown** or suspicious sources

Validate the sender identity for emails who ask you to take unconventional actions such as disclosing information, granting permissions, etc. – even if it is from well-known people, many spoofing and phishing attacks will take place these days

Try not to be distracted by Spam emails, try to use systems that detect such emails and remove them from your inbox – This is particularly detrimental to productivity but can also sometimes reveal your information to malicious hostiles

Send sensitive information by using only an **encrypted channel** – especially emails that are very vulnerable to man-in-the-middle attacks and other attacks that can expose you and your recipients information

Additional Precautions

- **Make sure the Wi-Fi is secured** (WPA2) and the WPS feature is disabled at the router – Wi-Fi Protected Setup (WPS) is vulnerable to Wi-Fi attacks which takes less than 5 minutes to get in the network
- **Use Anti-Virus/Anti-Malware** with the latest updates
- **Update** your Windows to the latest version
- **Remove unused applications** – especially the recent app for Coronavirus map which contains a malware
    a. See more at **https://www.scmagazine.com/home/security-news/malicious-coronavirus-map-hides-azorult-info-stealing-malware/**
    b. Disable any unknown/unused startup programs that runs at Windows boot

About Trustifi and No-Cost Email Security Licenses

Trustifi is offering no-cost licenses of its industry-leading email encryption solutions to help increase security amid a recent increase in telecommuters and home-based workers.

Trustifi is a cyber security firm featuring solutions delivered on a software as a service platform. Trustifi leads the market with the easiest to use and deploy email security products providing both inbound and outbound email security from a single vendor.

The licenses are being extended in light of travel bans and corporate policies enacted across the country, motivating many companies to ask a percentage of their staff to conduct business remotely. In this way, Trustifi hopes to help ease the transition during this challenging period, allowing virtual employees to transmit corporate emails in a more secure environment using 256-bit email encryption, data loss prevention and advanced threat protection.

Interested parties can use **this link** to engage a Trustifi representative who can get you started today.

There is no obligation to purchase.

Multi layered 360° Protection

256-Bit AES Encryption

NSA grade protection over your data and files

Extra Security Features

- One time access to files/emails
- Block access to print files
- Delete or edit messages after they have been sent

Inbound Protection

Stay protected from malicious links and files, viruses, phishing and spoofing attacks, ransomware attacks and even Spam.

Multi-Factor Authentication

on the recipient- You can choose to lock an email by adding a pin or a question that can only be unlocked by the intended recipient for an extra layer of protection

No Log-in Portal or Account Necessary

one click authenticate and decrypt allows your recipients to open your emails and also reply encrypted without ever having to sign up or login to anything

Trustifi hopes to help ease the transition during this challenging period, allowing virtual employees to transmit corporate emails in a more secure environment using 256-bit email encryption, data loss prevention and advanced threat protection.

www.trustifi.com
1-844-235-0084
info@trustificorp.com

Trustifi