REVALSYS
CREATING POSSIBILITIES

INFORMATION SECURITY TIPS
FOR REMOTE EMPLOYEES

Article from Revalsys Technologies

This article explains about the information security tips for remote employees

Working from home has become a norm after the outbreak of COVID-19 due to social distancing measures. It is expected to remain widespread even post-pandemic for convenience and health reasons.

Researches have shown that working from home increases the productivity of employees as they face fewer distractions and their commute time is saved. However, it poses a number of cybersecurity threats to them. When employees work from home, they may not have access to security measures that keep their data safe at work, which puts their privacy and the security of their companies at risk.

If you are a remote employee, you can ensure your work data is secure by taking the following precautions:

Use Strong Passwords

Passwords are essential to secure your accounts and devices. Strong passwords are a combination of lowercase and uppercase letters, numbers, and special characters. You must not use simple letter combinations like “qwerty” or common phrases/words like “password”, and simple numerical combinations like sequences or repeat numbers. They are very easy for hackers to crack. Other weak passwords are your name, date of birth, contact number, and other personal information. Create long passwords and remember not to use the same password for multiple accounts and devices.

Keep Changing Up Your Passwords

As important as it is to use strong passwords, it is equally crucial to change them in frequent intervals. One common mistake many employees make is using one password for a very long time. Changing passwords every three months is a good practice.

Use Different Passwords For Different Accounts And Devices

Coming up with a different password for a different account and device and remembering all the passwords is not easy but it is crucial for your security. Password reuse puts multiple accounts and devices at risk at a time. The risk is bigger when the password being used is a weak one.

Use Multifactor Authentication

Securing your accounts with just one strong password is not enough. Multifactor authentication involves verifying the identity of users through multiple ways before they log into an account. This method adds an extra layer of protection to accounts. Even if hackers get through one of these layers, they will be prevented by the rest of them.

Use A VPN

A VPN (Virtual Private Network) encrypts the information that is transmitted between employers and their employees. This makes the data difficult to access for those who try to intercept it. Remember to leave the VPN on throughout your office hours and switch it off after work, during commute time, etc.

Use Separate Devices For Personal And Official Purposes

Devices that are used for personal purposes lack security measures like antivirus and firewalls that are necessary to protect sensitive official data. You can secure the data by storing it on separate devices that are equipped with all the required security measures. Using a separate device for work also allows you to store it separately after work hours and ensure its safety.

Do Not Use Public Wi-Fi Networks

There is no firewall between you and the other users of public Wi-Fi networks. This makes it easy for them to hack your internet traffic and steal sensitive information. One solution to this is using your own mobile device’s personal hotspot. You also get the option to hide your hotspot from the public.

Create A Separate Workspace

When you work from home, the devices you use for work and the data on them are easily accessible to your friends and family. A simple and effective yet often overlooked way of securing official information and devices at home is allotting a separate area for work and setting up work equipment there.

Keep Your Official Devices Locked

Work-from-home offers employees the flexibility to work from not only their homes but also from public places like restaurants, libraries, etc. However, this advantage comes with its own challenge. Working outdoors means that your device and the data on it are exposed to strangers. You should secure your device with a password or a PIN so that if you have to leave it behind for a while you can lock it. Doing this encrypts the data on the device until you return and unlock it.

Install An Antivirus

Antivirus software is one that looks for, prevents, and eliminates viruses from devices. Once it is installed, it runs in the background to protect devices against viruses in real time. Initially designed for computers, antivirus now also protects mobile devices against viruses. The software also scans files traveling over the internet for threats and protects them from cybercriminals.

REVALSYS
CREATING POSSIBILITIES

CONTACTS

For more information on Revalsys Technologies, visit www.revalsys.com

8-2-293/82/1/83-A, 1st Floor,
Road No 12, Banjara Hills,
MLA Colony,
Hyderabad - 500034
Telangana, India

Phone: +91 7032660301

info@revalsys.com