OIC-CERT

Computer Emergency Response Team

Remote Working Security

Cybersecurity Awareness

WHAT IS REMOTE WORKING?

About Remote Working

Remote working is a method that allows an employee to work outside traditional working environment to carry out their day to day operational tasks.

Employees can either work using company provided devices or personal devices.

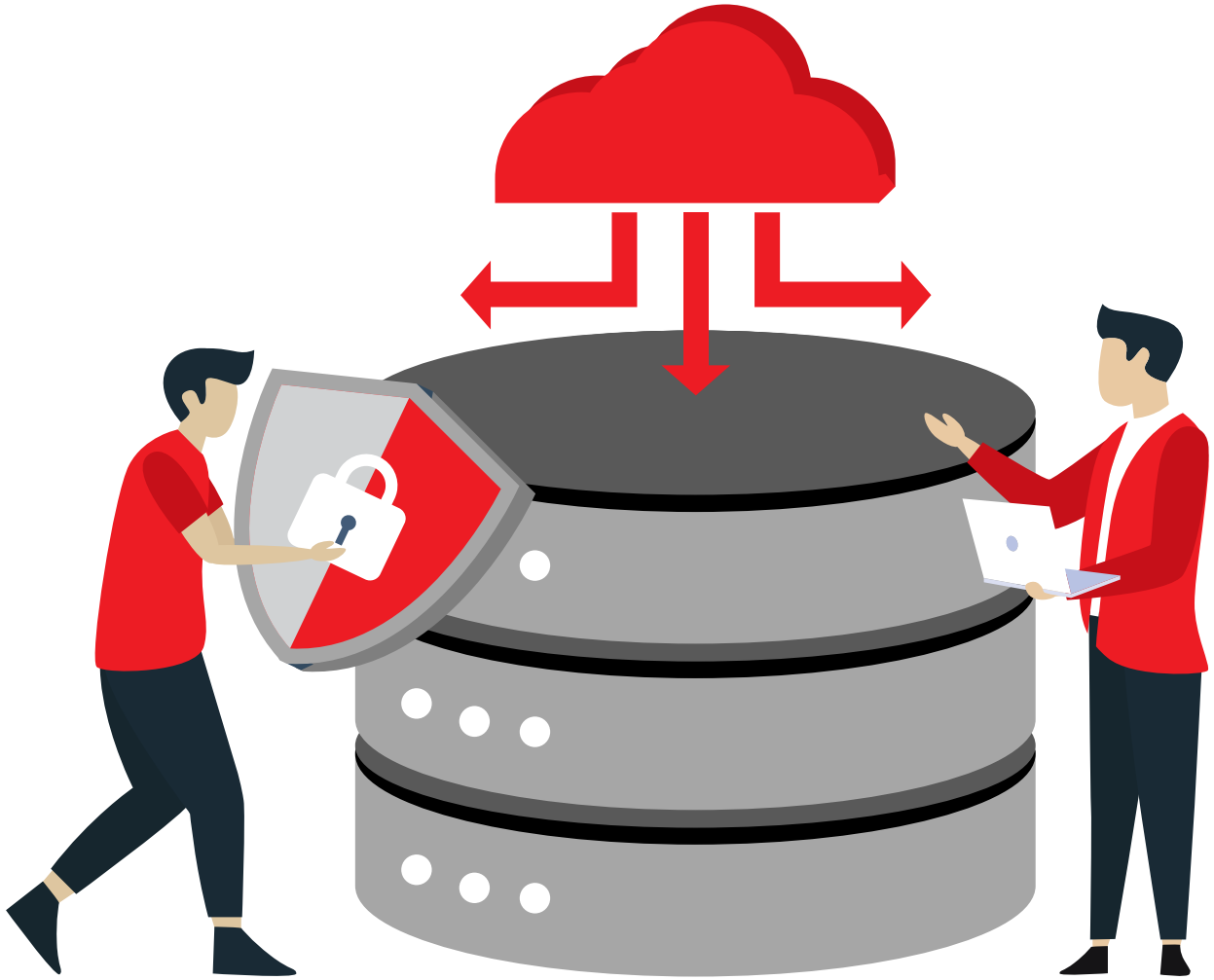
Remote Working Benefits

Keeping distance during the current pandemic situation.

Ensuring business continuity.

Ensuring customer happiness.

HOW TO ENSURE SECURITY WHILE WORKING REMOTELY?



Prepare a Dedicated Work Space

- It is preferred to have a dedicated, secure, and isolated work space at home or the remote site.
- Ensure the space is suitable for keeping company devices and documents.
- Set the right expectation for those around you.
- Be organized to avoid data loss.
- Be prepared for unexpected video calls and ensure wearing the formal attire.

Physical Security

Ensure physical protection of company devices or any devices containing company data.

Ensure protection against heat, dust, or theft.

Keep company files away from kids and pets in a secure location.

Lock It to Protect It

Lock your devices when away using the Windows key + L.

You can physically lock the dedicated workspace if possible.

Be aware of shoulder surfing in public places.

Avoid Sharing

Companies prohibit employees from sharing company provided devices with family members or friends.

Never share company classified data with unauthorized individuals.

Avoid Personal Use

Use company provided devices for work related activities only.

Do not install any applications that are not work related on company devices

Refrain from using personal USB drives on work devices.

Email Security

- Do not use personal emails for work purposes.
- Use end-to-end encryption by enabling the hosted S/MIME under settings.
- Restrict from using the “reply-to-all” function.
- Do not click on suspicious links in emails, known as phishing emails, even if received from a mutual source.
- Always verify the sender before replying.
- Scan all attachments for viruses and malware infections.

Use a Secure Connection

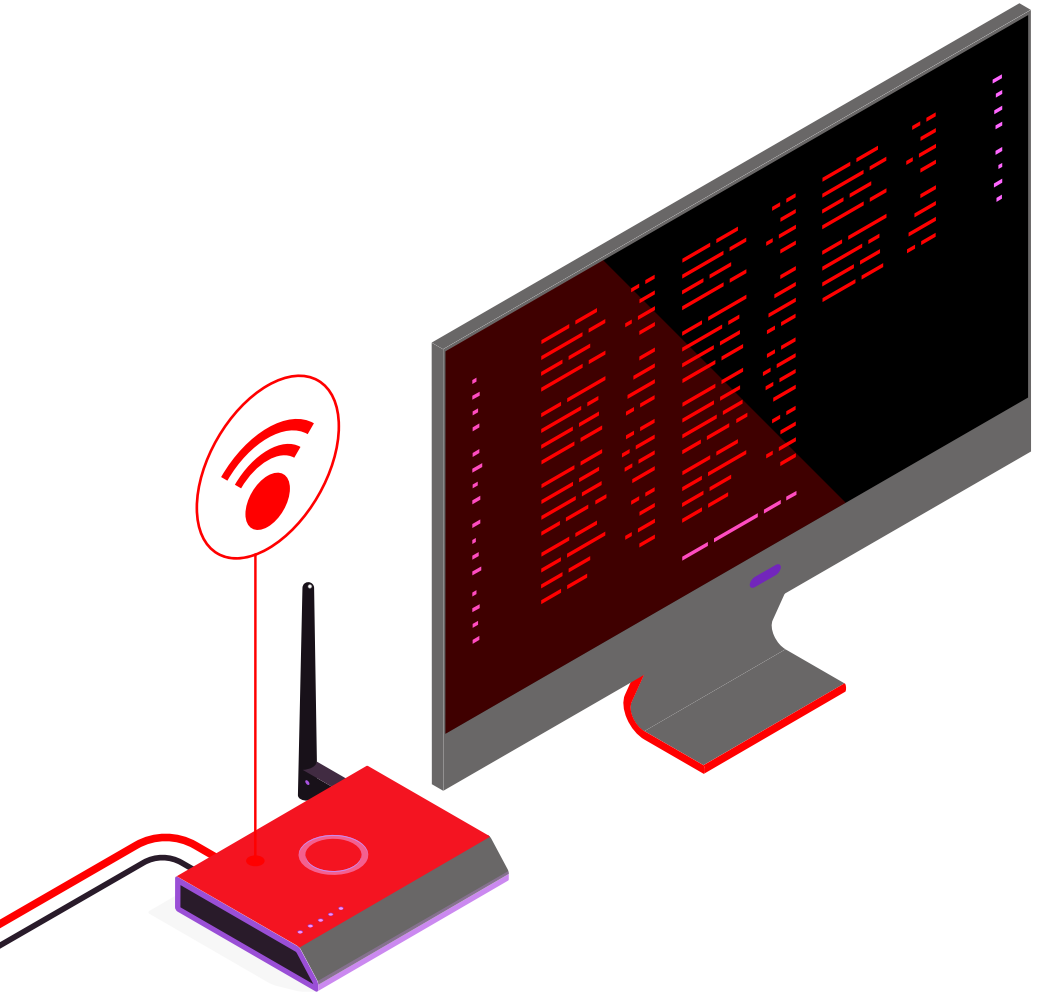
Connect using the approved virtual private network (VPN) client from your company (if provided).

Do not use open public Wi-Fi for completing business tasks.

Ensure securing your home Wi-Fi.

Do not connect to untrusted Wi-Fi connections.

Secure Your Home Wi-Fi



Forget or remove the Wi-Fi settings for your network from any devices that connect to your Wi-Fi router such as laptop, mobiles, gaming consoles, TVs, etc.

Do the following changes in the router settings:

- Make sure that your Wi–Fi router's firmware is up to date. “The settings will display if older version”
- Set a unique SSID or Wi-Fi name.
- Hide the SSID and make it a hidden network.
- Set a unique and strong password.
- Set to WPA2 or WPA3 to strengthen/ protect your Home network

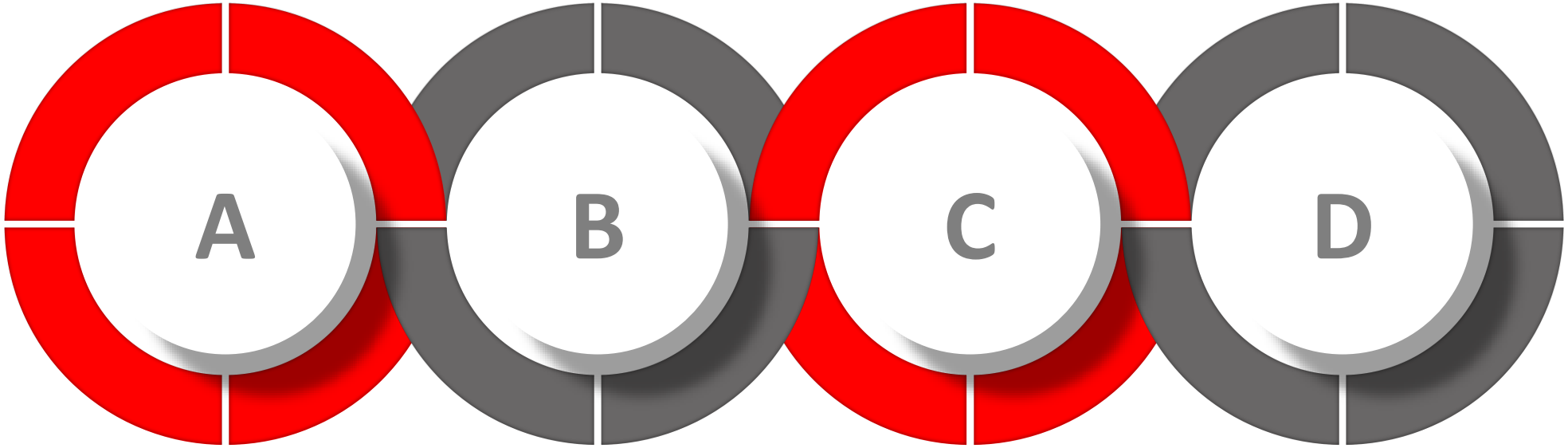
Use a Strong First Line of Defense

Start with a passphrase

I Love Chocolate

Add Special Characters

1 L0v3 C#0c0l@t3



Add Numbers

1 L0v3 Ch0c0lat3

Mix uppercase and lowercase

1l0V3c#0C0L@t3

Never Share Your Identity

Never share your passwords with friends and family members.

Never write down your password.

Avoid using the same passwords for different accounts.

Use Two Factor Authentication

Set up two-factor or multi-factor authentication or verification to add an extra layer of protection to all your accounts.

Examples: Verification via email or a text message, random secure token, biometric method such as facial recognition or a fingerprint scan, etc.

Video Conference

- ✓ Use only trusted or company approved video conferencing or information sharing platforms/ tools that allow employees to chat, host audio, video, and web conferences online.
- ✓ Do not use work-related Collaboration Tools for personal use.

Online Collaboration

- Always scan the files with an up to date Antimalware program before sharing.
- Do not share files from unknown sources.
- Do not accept any invitations from unknown users.
- Report any suspicious activity to your system administrator immediately.
- Do not record or screenshot conversation without all parties' permission.
- For meetings that require the enabling of the webcam, please ensure you are following the official dress code.

Secure Your Collaboration Tools

- Enable waiting rooms.
- Require a password for joining.
- Do not use a personal meeting ID.
- Lock the meeting.
- Disable file transfer.
- Allow screen sharing for host only.

Use Approved Cloud Applications

Using cloud approved applications enables to store business data and information under a cloud that’s accessible only by authorized employees.

Example: Microsoft, Office 365, OneDrive, etc.

Download Approved Applications

Employees must inform the respective department of any installation of applications.

Approval must be taken prior to any downloads.

Don’t Be Scammed

Social engineering scams: Manipulation of the natural human tendency to trust. Victims are requested to provide information or to take an action.

Phishing scams: Social engineering over email where attackers try to scam users by sending emails pretending to be from a legitimate entity.

Others communication technologies and tools can also be used for scamming users such as SMS, phone, video conferencing tools, social media, etc.

Beware of Cyber Attacks

Beware of phishing attacks targeting employees with COVID-19 related information

Never click on links/download attachments in suspicious emails and report the incident to the appropriate department immediately.

Distributed via the CDC Health Alert Network
February 4, 2020
CDCHAN-00426

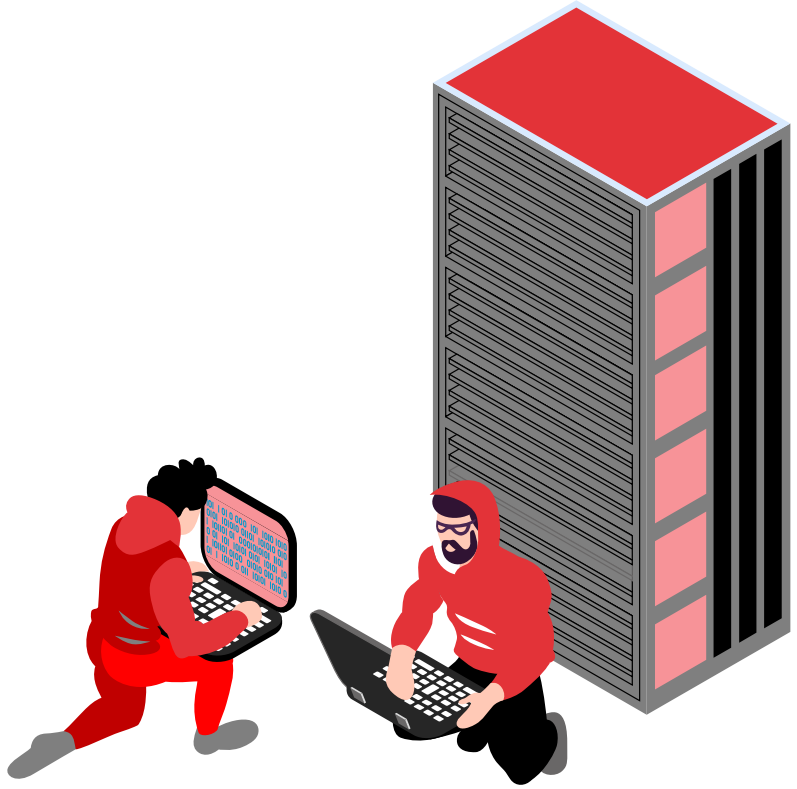
Dear [redacted]

The Centers for Disease Control and Prevention (CDC) continues to closely monitor an outbreak of a 2019 novel coronavirus (2019-nCoV) in Wuhan City, Hubei Province, China that began in December 2019. CDC has established an Incident Management System to coordinate a domestic and international public health response.

Updated list of new cases around your city are available at (https://www.cdc.gov/coronavirus/2019-nCoV/newcases-cities.html)

You are immediately advised to go through the cases above to avoid potential hazards.

Phishing email from U.S. Centers for Disease Control and Prevention.



Information Exchange & Transfer

Use company approved channels for exchanging information and transferring files.

Choose the communication channel based on the classification level of the information being shared or exchanged.

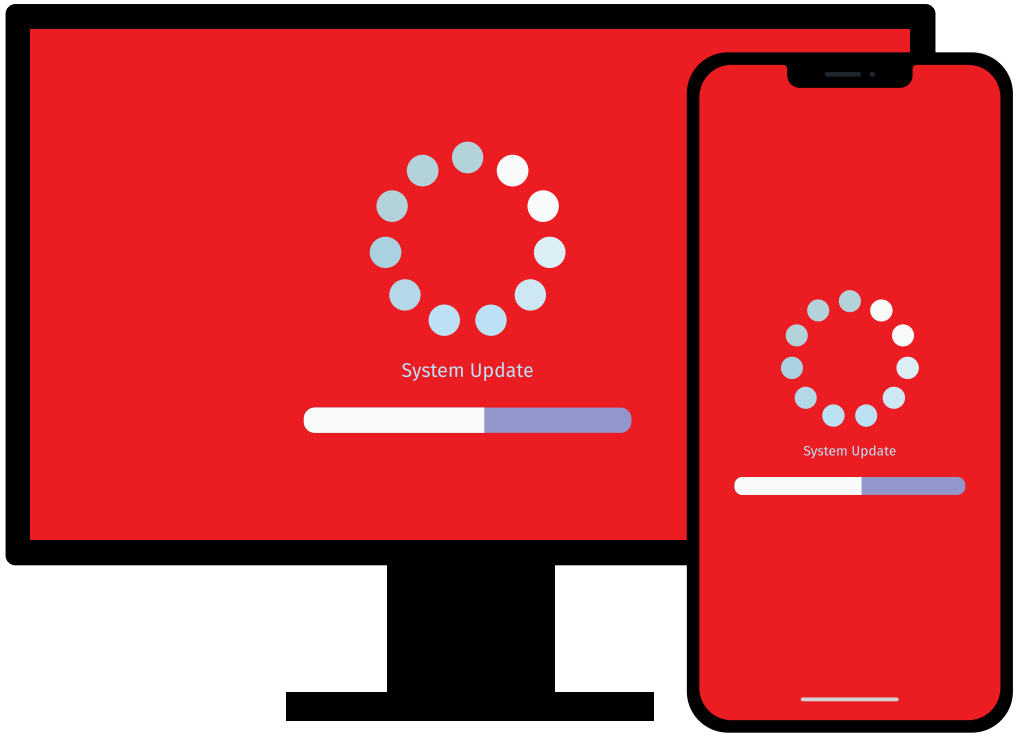
Information Exchange & Transfer

Keep business documents or information on the company's shared drive to avoid any data loss and to enable IT to take backups.

Install Updates Regularly

Do not ignore any reminders or notifications regarding software and device updates.

Set your device to run updates automatically.



Secure Your Personal Devices

Update your operating system and software regularly.

Use a trusted and up to date antimalware software.

Backup your data in a secure location.

Install applications only from trusted sources.

Use a desktop firewall.

Comply with Policies and Procedures

Read, understand, and comply with company policies and procedures while working remotely.

Reporting Incidents

Report any work related information security incidents to the IT helpdesk.

Report personal security incidents to the local authorities and the police.

Questions?


WHAT? HOW? WHEN?
WHO? WHERE? WHO?
WHEN? WHY? WHAT?
WHY? HOW?
WHERE? WHO?
HOW? WHAT? WHERE?
WHO? WHERE? WHO? WHY? HOW?
WHAT? HOW? WHERE?
WHO? WHY? WHAT?
WHERE? WHEN?
WHAT? WHO?
WHERE? WHO?
HOW? WHAT?
WHO? WHERE?
WHY? WHAT? HOW?
HOW? WHO? WHEN?
WHAT? WHERE?
WHY? WHEN? WHAT?
WHERE? WHO? WHY? HOW?
HOW? WHERE?
WHAT? WHY?
WHEN? WHO? WHAT?
WHERE? WHAT? HOW?
WHO? WHY? WHERE?
WHAT? WHEN?


WHERE?
WHO? WHAT?
WHERE? WHY?
HOW? WHEN?
WHAT? WHO?
WHEN?
WHY? WHERE?
WHEN? HOW?
HOW? WHERE? WHO? WHAT?
WHY? WHAT? WHEN?
WHERE? HOW?
WHAT?
WHEN? WHO?
WHERE?