Unleashing Values

IREL(India) limited

(A Govt. of India Undertaking)

DO'S AND DONT'S FOR INTERNET & IT INFRATRUCTURE SECURITY

FOR IREL's INTERNAL USE ONLY

DISCLAIMER

This IT Guidelines serves as a reference guide for employees, outlining the best practices and guidelines for maintaining internet and infrastructure security within the organization. The contents of this guidelines are for informational purposes only.

While every effort has been made to ensure the accuracy, consistency, and completeness of the information provided in this guidelines, the organization does not assume any legal liability for the accuracy, completeness, or usefulness of the contents. In case of any conflict between the guidelines and the organization's official IT policies, security protocols, or applicable government regulations/instructions, the latter will take precedence.

Any information provided herein should not be cited in any legal disputes or litigation, nor does it replace any formal legal interpretation or evidence. Employees will be solely responsible for any consequences resulting from decisions made based on the information contained in this guidelines.

The contents of these guidelines are strictly for IREL’s internal consumption and shall not be shared with any external entity of any form.

Furthermore, please note that the IT department will not entertain direct requests for clarification or references related to the contents of this guidelines from employees. Any such queries should be directed to the relevant department or office, which will, through the proper channels, escalate the matter to the Chief Information Security Officer (CISO).

(For further assistance or inquiries, please reach out to Nirdesh Kumar Sharma, Chief Information Security Officer (CISO), at nirdesh.sharma@irel.co.in or contact on 8104997149)

CONTENTS

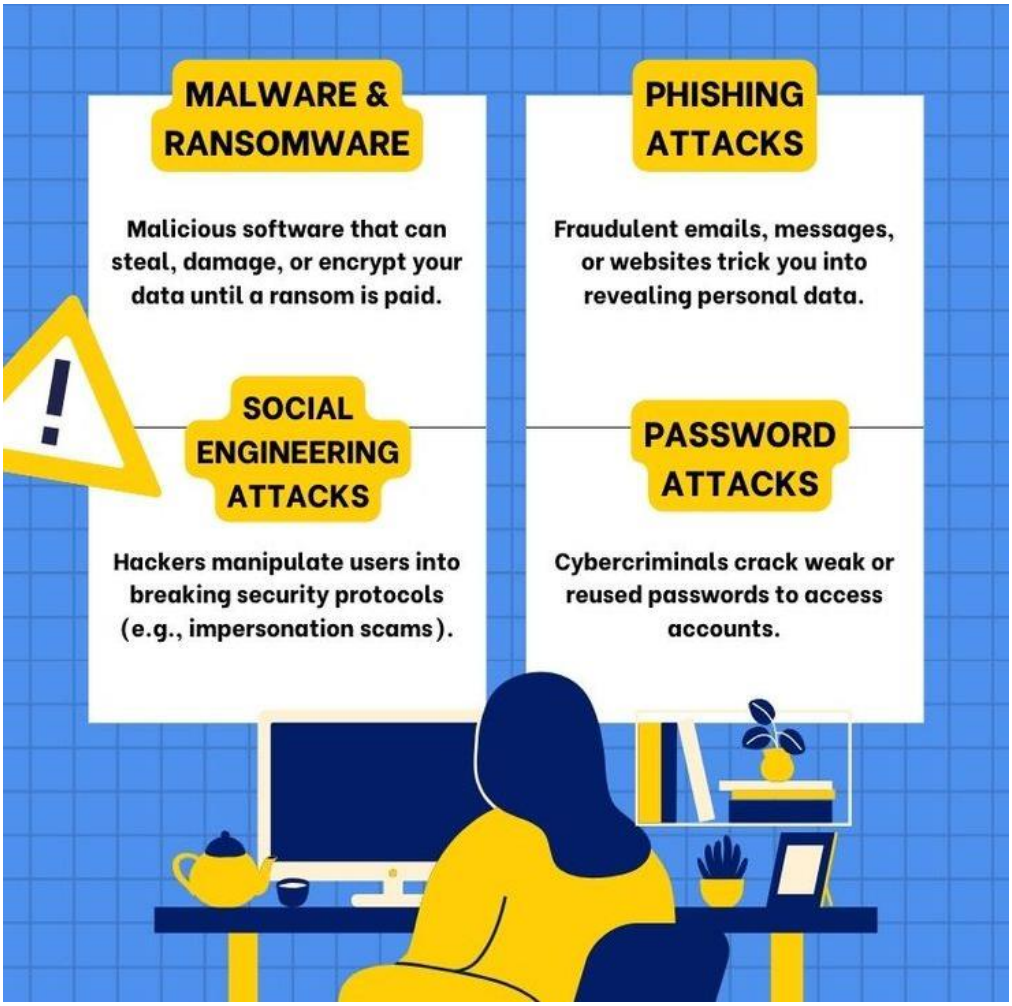
"Empowering Individuals: Your Guide to Stay Cybersecure in a Digital World"

INTRODUCTION

As a leading PSU, securing our network and infrastructure is crucial for protecting national assets, ensuring continuous service, and maintaining public trust. The following MEASURES are strategic necessities to enhance our defense against evolving cyber threats.

COMMON CYBER ATTACKS

CYBER ATTACKS



Attack Type	Description	Example
Phishing	Phishing attacks try to trick you into giving away sensitive information, like passwords or bank details, by pretending to be a trusted source.	You might receive an email asking you to click a link and enter your login info, giving attackers access to company systems and causing serious financial damage.
Malware	Malware is harmful software that can steal or lock your files. It usually comes from unsafe downloads or fake updates.	A fake software update could install ransom ware that locks important company data, causing financial losses and damaging the company's reputation.
Password Attacks	Password Attacks occur when cybercriminals attempt to gain unauthorized access by exploiting weak or stolen passwords.	A cybercriminal gains unauthorized access to a user's account because the user's password is weak and easily guessable, like "123456." The attacker quickly enters this password and successfully logs into the account.
Ransomware	Ransomware locks files and demands payment to restore access, halting business operations.	A ransomware attack could lock client-facing systems, causing financial damage, loss of client trust, and potential legal issues due to exposed sensitive data.
Social Engineering Attacks	Manipulate people into revealing confidential information or performing actions that compromise security.	A phishing email that tricks someone into sharing their login details by pretending to be from a trusted source.

HOW TO RECOGNIZE CYBER ATTACKS

How To Recognize Cyber Attacks

Unusual Emails or Messages:

Any email or message that looks suspicious, with generic greetings or unexpected attachments, should be treated with caution. These may be attempts to steal sensitive information or introduce harmful files to our systems.

Suspicious Pop-Ups:

Pop-ups claiming your device is infected or warning of an emergency are usually designed to trick you into clicking harmful links or downloading malware, which can damage company systems.

Unrecognized Login Attempts:

If you receive alerts about login attempts from unknown devices or locations, it could mean unauthorized access attempts are being made, signaling a potential cyber-attack.

Unusual File Changes:

Files that disappear, change names, or behave oddly (like crashing or corruption) may indicate malware or an ongoing attack, risking important company data.

Unfamiliar Software:

The appearance of unknown apps or programs on your device could suggest malware has been secretly installed, compromising both personal and company data.

HOW TO STAY SAFE ONLINE

Enable Multi-Factor Authentication (MFA):
Enhance security by adding an extra verification step when logging into your accounts.

Keep Your Software Updated:
Stay on top of updates, as they often include important security patches. Make sure to install them promptly.

Be Cautious on Public Wi-Fi:
Avoid accessing sensitive accounts over public Wi-Fi unless you're using a VPN to secure your connection.

Backup Your Data Regularly:
Use secure cloud services or external drives to store important files so you can recover them if needed.

Think Before You Click:
Refrain from clicking on suspicious links or downloading attachments from unfamiliar sources.

ENABLE MULTI-FACTOR AUTHENTICATION (MFA)

Add an extra layer of security by requiring a second verification step, like a code or biometric scan.

BACKUP DATA REGULARLY

Protect important files by storing backups on secure cloud services or external devices.

SECURE YOUR NETWORK

Use firewalls, strong Wi-Fi encryption, and a reliable VPN to safeguard your internet connection.

KEEP SOFTWARE UPDATED

Regularly update your operating systems and applications to patch vulnerabilities and protect against cyber threats.

MANAGING GOOGLE PERMISSIONS FOR WORK EFFICIENCY AND SECURITY

1. **Location Access**:
    - **Impact on Work**: If Google constantly tracks your location, it can drain battery life, reduce device performance, and create unnecessary notifications. This can distract you during work hours and reduce your productivity.
    - **Solution**: Keep location services on only when needed (for meetings, work-related travel) and turn it off when not in use to save battery and maintain focus.
2. **Contacts Access**:
    - **Impact on Work**: Allowing Google full access to your contacts can cause accidental sharing of professional information (e.g., email addresses, phone numbers) with third-party apps or services.
    - **Solution**: Only grant contacts access to apps that require it for work purposes (like email or calendar apps) and avoid syncing contacts unless absolutely necessary.
3. **Camera and Microphone Access**:
    - **Impact on Work**: If camera or microphone access is given to unnecessary apps, this could lead to unwanted distractions or interruptions during meetings. It can also create security vulnerabilities where malicious apps could eavesdrop or record without permission.
    - **Solution**: Limit camera and microphone access to apps like Google Meet or Zoom for work meetings only. Disable access for other apps unless needed.
4. **Personal Data Syncing**:
    - **Impact on Work**: Syncing personal and work-related data across devices can lead to confusion, mixing personal contacts, calendars, and emails with professional data, making it harder to keep work separate and organized.
    - **Solution**: Use separate Google accounts for personal and work use. Only sync work-related data to avoid cross-contamination of personal and professional information.
5. **Storage Permissions**:
    - **Impact on Work**: Google’s access to your device's storage can lead to unintentional upload of sensitive or personal files, or misuse of documents that should remain confidential.
    - **Solution**: Only grant Google storage access for work-related documents or files. Regularly check the permissions and file uploads to avoid mishandling confidential information.

DO'S: ACTIONS TO STRENGTHEN SECURITY

Ensure Role-Based Access Control (RBAC):

Limit system access to what's needed for your role. Once your task is complete, revoke access to sensitive systems.

- **Example:** As a System Designer, once the design phase is completed, your access to operational systems should be revoked to prevent unauthorized access.
- **Impact:** Unauthorized access can lead to data breaches, loss of customer trust, and financial losses.

Participate in Security Training and Awareness Programs:

Engage in training to learn how to protect data and recognize security threats like phishing.

- **Example:** Learn to recognize phishing emails, such as suspicious links or unusual requests for sensitive information.
- **Impact:** Failure to recognize security threats can expose the organization to cyber-attacks, leading to significant financial and reputational damage.

Follow Strong Authentication Practices:

Use strong, unique passwords and enable Multi-Factor Authentication (MFA) when possible (e.g., at least 12 characters with a mix of letters, numbers, and symbols).

- **Example:** Enable MFA for systems with access to sensitive data, requiring both a password and a secondary verification method (e.g., a mobile code).
- **Impact:** Weak passwords increase the risk of unauthorized access and data breaches.

Regularly Update Credentials:

Change your passwords every 90 days and ensure that they are unique across different platforms.

Never share your passwords or login details, even if someone claims to be from IT or management.

- **Example:** Update passwords for OT (operational technology) systems quarterly.
- **Impact:** Stale passwords can be exploited, risking security.

Stay Alert for Social Engineering Attacks:

Always verify the identity of anyone requesting sensitive data, especially by email or phone.

- **Example:** Validate the identity of anyone asking for credentials before sharing.
- **Impact:** Falling for social engineering can lead to data breaches and financial losses.

Maintain Data Privacy and Confidentiality:

Protect sensitive company and client data. Follow privacy policies and legal regulations when handling both digital and physical information.

- **Example:** Don't discuss sensitive data in public and lock your computer when away.
- **Impact:** Mishandling data can lead to legal issues, reputational harm, and loss of trust.

Ensure Secure Remote Working:

Use a VPN and company-approved devices when working remotely. Avoid personal devices for accessing corporate systems.

- **Example:** se encrypted Wi-Fi at home and avoid public Wi-Fi for accessing critical systems.
- **Impact:** Unsecure remote access can expose company data to cyber threats and financial loss.

Secure Personal Devices:

Ensure personal devices used for work (smartphones, laptops) are protected with strong passwords, biometric security, and encryption.

- **Example:** Secure your phone with a PIN and encryption if accessing work emails.
- **Impact:** Compromised devices can serve as entry points for cyber threats.

Handle Physical Security with Caution:

Always lock up devices, physical records, and security assets when not in use.

- Example: Lock away sensitive documents and store electronic devices securely when away from your workstation.
- Impact: Theft of devices or documents can lead to data breaches and unauthorized access.

DONT'S: PRACTICES TO AVOID AT ALL COSTS

Don't Underestimate External Threats:

Be aware that activists or external threats may target vulnerable employees to access company systems or data.

- **Example:** Be cautious of suspicious requests for internal information or system access from unknown sources.
- **Impact:** External threats could cause reputational damage, disrupt operations, or leak sensitive information.

Don't Use Unsecured Networks for Work:

Avoid accessing company systems or data over unsecured networks or personal devices.

- **Example:** Don't log into internal systems via public Wi-Fi without a VPN.
- Im**pact:** Unsecured networks can expose data to hackers, risking a breach or theft of confidential information.

Don't Share Sensitive Information with Untrusted Sources:

Never disclose sensitive company information to unauthorized persons, even if they seem legitimate.

- **Example:** Share system access details only with approved contractors who require them.
- **Impact:** Sharing confidential info with untrusted sources can lead to unauthorized access and data leaks.

Don't Leave Workstations Unattended Without Locking:

Always lock your workstation when leaving your desk, especially when accessing sensitive data.

- **Example:** Lock your computer screen when stepping away from your desk.
- **Impact:** Unattended workstations can be exploited for unauthorized access or data theft.

Don't Overlook the Importance of Secure File Sharing:

Use secure, approved methods for sharing sensitive files, avoiding unsecured options like email.

- **Example:** Use the organization's encrypted file-sharing platform for sensitive data.
- **Impact:** Unapproved sharing methods can expose files to unauthorized access or hacking.

Don’t Assume IT Security Is Only IT’s Responsibility:

Cyber security is everyone’s responsibility. Report any suspicious activity or security concerns immediately.

- **Example:** Inform IT if you notice unusual system behavior or security threats.
- **Impact:** Delayed reporting can allow threats to escalate and compromise company systems.

Don’t Neglect Personal Device Security:

Secure personal devices used for work and ensure compliance with company policies.

- **Example:** Install anti-virus software and keep devices updated to protect against malware.
- **Impact:** Unsecured personal devices can introduce cyber threats into company systems.

Don’t Disregard Secure Remote Working Practices:

When working remotely, always use secure connections and tools provided by the organization.

- **Example:** Use VPN and Multi-Factor Authentication (MFA) when accessing company data remotely.
- **Impact:** Lack of proper security during remote work can expose company data to unauthorized access.

Don’t Use Personal Passwords for Work Systems:

Keep work passwords separate from personal accounts, and use strong, unique passwords.

- **Example:** Set unique passwords for work systems and avoid reusing them across platforms.
- **Impact:** Reusing passwords makes systems vulnerable to breaches and data loss.

DO'S FOR MOBILE APPLICATION SECURITY:

Use Secure Communication Channels (e.g., HTTPS):

Always ensure that mobile apps use HTTPS for transmitting sensitive data. This encryption protects against unauthorized access and man-in-the-middle attacks during communication.

- **Example:** Ensure login details, payment information, and personal data entered in the app is sent securely via HTTPS.
- **Impact:** Unencrypted communications can expose sensitive data to interception and unauthorized access.

Encrypt Data at Rest and In Transit:

Make sure that both stored and transmitted data is encrypted. This protects user credentials, personal information, and payment details from unauthorized access.

- **Example:** Use secure storage methods like iOS Keychain or Android Keystore for sensitive data and ensure encryption is used when transmitting data.
- **Impact:** Unencrypted data is vulnerable if the device is compromised or during transmission.

Safeguard Personal Devices with Encryption:

Ensure employees use device encryption to protect data on personal mobile devices. This makes it harder for unauthorized users to access sensitive information if the device is lost or stolen.

- **Example:** Recommend full disk encryption and remote wipe features on personal mobile devices used for work purposes.
- **Impact:** Unencrypted devices can expose sensitive data if lost or stolen.

Follow Organizational Security Policies for Data Encryption:

Ensure mobile apps comply with the company's encryption policies, which are designed to protect sensitive data and meet industry regulations (e.g., GDPR, HIPAA).

- **Example:** Align app encryption methods with company policies for cloud storage or Third-party service integration.
- **Impact:** Failing to comply with encryption policies can lead to data breaches and regulatory non-compliance.

Encrypt Backup Data and Storage Devices:

Encrypt backup data, including logs and user information, to protect it from exposure if lost or stolen. This applies to both cloud and external storage devices.

- **Example:** Ensure data synced to cloud services or stored on external devices is encrypted before being uploaded or stored.
- **Impact:** Unencrypted backup data can be compromised if the storage device is lost or accessed by unauthorized individuals.

DONT'S FOR MOBILE APPLICATION SECURITY:

Don't Skip Secure OS Features:

Mobile OS features such as app sandboxing, secure data storage, and encryption are essential for protecting apps from unauthorized access. Disabling or bypassing these features increases security risks.

- **Example:** Failing to enable security features like automatic updates and firewalls on an operating system can leave it vulnerable to attacks, without these protections, an attacker could exploit known vulnerabilities to gain unauthorized access to the system.

Don't Use Unverified Third-Party SDKs:

Using unverified or insecure third-party SDKs can introduce vulnerabilities or backdoors, compromising app functionality and user data.

- **Example:** Integrating an untrusted SDK could allow attackers to gain access to sensitive data or compromise the app's security.

Don't Over-Permit Your Applications:

Requesting excessive permissions, like access to contacts, camera, or microphone, increases security risks and exposes user data. Only request permissions necessary for core functionality.

- **Example:** An app with excessive permissions led to privacy violations, exposing users' private moments.

Don't Use Deprecated or Outdated Libraries:

A breach exposed financial data due to the use of an outdated library with known vulnerabilities.

- **Example:** An attacker could exploit a known flaw in an outdated library to gain unauthorized access to the application.

Don't Store Data Unencrypted on Backup Systems:

Storing unencrypted backup data makes it vulnerable to unauthorized access if the backup system is compromised. Always encrypt backup data.

- **Example:** If an attacker gains access to an unencrypted backup, they could easily steal sensitive information like customer data or company secrets.

DO'S FOR SOFTWARE PROTECTION:

Action	Description	Example
Do Regularly Update Software	Keep software, operating systems, browsers, and applications updated to close vulnerabilities. Cybercriminals exploit outdated software to gain unauthorized access.	An attacker could exploit an unpatched security flaw in outdated software to gain unauthorized access to your system.
Do Use Antivirus and Anti-malware Tools	Ensure devices are equipped with up-to-date antivirus and anti-malware software to detect and remove malicious threats.	Do Use Antivirus and Anti-malware Tools, which could lead to stealing financial data and causing operational delays.
Do Implement Access Controls and Least Privilege	Adopt access controls and the principle of least privilege, ensuring users can only access the data necessary for their tasks.	If an employee has access to data they don't need for their role, an attacker could exploit that access to steal or manipulate information, exposing millions of customer records.
Do Use Strong Passwords and MFA	Enforce strong password policies and enable multi-factor authentication (MFA) to add an extra layer of security.	A breach can occur due to weak passwords, compromising sensitive user data and costing the company millions in fines and reputation damage.
Do Regularly Backup Data	Ensure regular backups of critical data to mitigate the impact of cyber-attacks or accidental loss. Periodically test backup systems for reliability.	A ransom ware attack could force a company to pay a ransom because they lacked regular backups, resulting in millions of dollars in losses.

DONT'S FOR SOFTWARE PROTECTION:

Action	Description	Example
Don't Ignore Security Vulnerabilities	Always report security vulnerabilities to avoid exploitation by cybercriminals.	A retailer ignoring an app vulnerability may lead to breach and customer data loss.
Don't Use End-of-Life (EOL) Software	Avoid using outdated software that no longer gets security updates.	Using unsupported software may led to breach and exposed customer data.
Don't Trust Unknown Software	Don't install unverified software that could contain malware.	Unverified software may cause a breach by stealing user credentials.
Don't Share Sensitive Information Over Unsecure Channels	Always use secure methods to share sensitive data.	Sending data via unsecure email may led to a breach and financial loss.
Don't Download Apps from Untrusted Sources	Only download apps from trusted sources to prevent malware infections.	A malware-infected app can stole customer data, causing financial loss.

DO'S FOR EMAIL PROTECTION:

Action	Description	Example
Do Use Email Security Protocols	Implement email security protocols to prevent spoofing and protect against fraud and data breaches.	An attacker could send an email pretending to be from your company, tricking employees into sharing login credentials.
Do Be Cautious with Email Attachments and Links	Always verify the sender before opening attachments or clicking on links, especially if the email seems unusual.	You receive an email with an unexpected attachment and link. Before opening, you verify with the sender, discovering it's a phishing attempt designed to install malware.
Do Implement Email Encryption	Encrypt emails containing sensitive information to protect data from being intercepted.	A breach can happen due to unencrypted emails containing sensitive data.

DONT'S FOR EMAIL PROTECTION:

Action	Description	Example
Don't Use Weak Email Passwords	Avoid using weak or reused passwords for email accounts to prevent unauthorized access to sensitive data.	Weak passwords could lead to a public leak of private data, resulting in reputational and financial harm.
Don't Ignore Email Security Alerts	Always respond promptly to security alerts to prevent potential breaches and data theft.	If you receive an alert about an unusual login attempt to your email account and ignore it, an attacker could gain unauthorized access and compromise sensitive data.
Don't Share Credentials via Email	Never share sensitive credentials through unsecured channels like email. Use encrypted methods instead.	If an employee shares unencrypted email credentials could lead to a data breach and millions in losses.