CEIA/5519/2024-IT

ചീഫ് എഞ്ചിനീയറുടെ കാര്യാലയം
പ്ലാനിംഗ് & ഐ.ടി.സെൽ,
പബ്ലിക് ഓഫീസ്, തിരുവനന്തപുരം -695033
ഇമെയിൽ itcellirrigation@gmail.com
തീയതി : 31-05-2025

സർക്കുലർ

വിഷയം: ജലേസചനം-സൈബർ സുരക്ഷ-Cyber Hygiene Practices for Government Employees- സംബന്ധിച്ച്.

സൂചന: കമ്പ്യൂട്ടർ എമർജൻസി റെസ്പോൺസ് ടീം കേരളയുടെ 09.05.2025 ലെ ഇമെയിൽ സന്ദേശം

മേൽ സൂചന പ്രകാരം എല്ലാ സർക്കാർ ജീവനക്കാരും അനുവർത്തിക്കേണ്ട സൈബർ സുരക്ഷാ സമ്പ്രദായങ്ങൾ ഇതോടൊപ്പം ഉള്ളടക്കം ചെയ്തത് എല്ലാ ജീവനക്കാരുടെയും അറിവിലേക്കായി നൽകുന്നു. ആയത് എല്ലാ ജീവനക്കാരും കൃത്യമായും പാലിക്കേണ്ടതാണ് എന്നും അറിയിക്കുന്നു.

ഉള്ളടക്കം: Cyber Hygiene Practices for Government Employees

Signed by Sreedevi P
Date: 31-05-2025 10:23:04

ചീഫ് എഞ്ചിനീയർ
(പൂർണ്ണ അധിക ചുമതല)

പകർപ്പ്:-

എല്ലാ കാര്യാലയ മേധാവികൾക്കും (വെബ്സൈറ്റ് മുഖേന)

IT Security Advisory: Cyber Hygiene Practice for Government Employees

OVERVIEW

This advisory outlines essential security measures that must be followed to minimize the risk of phishing attacks and malware infections across the IT infrastructure. It is being issued to alert the government employees to a rise in phishing scams that exploit panic during times of crisis, as cybercriminals are using emergencies to deceive individuals into disclosing sensitive information.

RECOMMENDATION

DESKTOP/LAPTOP AND PRINTER SECURITY AT OFFICE

- Use only Standard User (non-administrator) account for accessing the computer/laptops for regular work. Admin access to be given to users with approval of CISO only.
- Set Operating System updates to auto-updated from a trusted source.
- Always lock/log off from the desktop when not in use also shut down the desktop before leaving the office.
- Do not write passwords, IP addresses, network diagrams or other sensitive information on any unsecured material (ex: sticky/post-it notes, plain paper pinned or posted on users table etc.).
- Remove pirated /unsupported Operating systems and other software/applications that are not part of the authorized list of software.
- Enable Desktop Firewall for controlling information access.

PASSWORD MANAGEMENT

- Use complex passwords with a minimum length of 8 characters, using a combination of capital letters, small letters, numbers and special characters.
- Change passwords at least once in 120 days.
- Use Multi-Factor Authentication, wherever available to all your email, social media accounts etc.
- Don’t use the same password in multiple services/websites/apps.
- Don’t save passwords in the browser or in any unprotected documents

INTERNET BROWSING SECURITY

- While accessing Government applications/services, email services or banking/payment related services or any other important application/services, always use Private Browsing/Incognito Mode in your browser.

- Use the latest version of the internet browser and ensure that the browser is updated with the latest updates/patches.
- Don't store any usernames and passwords on the internet browser.
- Don't store any payment related information on the internet browser
- Don't use your official systems for installing or playing any Games
- Observe caution while opening any shortened URLs (ex: tinyurl.com/ab534/). Many malwares and phishing sites abuse URL shortener services. Such links may lead to a phishing/malware webpage, which could compromise the device.

MOBILE SECURITY

- Ensure that the mobile operating system is updated with the latest available updates/patches.
- Keep the Wi-Fi, GPS, Bluetooth, NFC and other sensors disabled on the mobile phones. They may be enabled only when required. Avoid using public Wi-Fi for accessing email or entering sensitive information unless using a secure VPN.
- Download Apps from official app stores of Google (for android) and apple (for iOS).
- Before downloading an App, check the popularity of the app and read the user reviews.
- Note down the unique 15-digit IMEI number of the mobile device and keep it offline. It can be useful for reporting in case of physical loss of mobile device.
- Take regular offline backup of your phone and external/internal memory card.
- Report lost or stolen devices immediately to the nearest Police Station and concerned service provider.
- Disable automatic downloads in your phone.
- Always keep an updated antivirus security solution installed.

EMAIL SECURITY

- Do not open attachments in unsolicited e-mails, even if they come from people in your contact list. Never click on a URL contained in an unsolicited e-mail, even if the link seems genuine.
- Never respond to unsolicited emails that request sensitive information like login credentials, financial details, or Social Security numbers.
- Check the integrity of URLs before providing login credentials or clicking a link. Do not submit personal information to unknown and unfamiliar websites.
- Never submit confidential information via forms embedded within email messages. Senders are often able to track all information entered.
- In cases of genuine URLs, close the e-mail and go to the organization's website directly through browser's address bar.
- Beware of emails and Web Pages providing special offers like winning prize, rewards, cash back offers etc.
- Do not share the email password or One auth OTP with any unauthorized persons.

SOCIAL MEDIA SECURITY

- Limit and control the use/exposure of personal information while accessing social media and networking sites. Always check the authenticity of the person before accepting a request as friend/contact.
- Use Multi-Factor authentication to secure the social media accounts.
- Do not click on the links or files sent by any unknown contact/user.
- Do not publish or post or share any internal government documents or information on social media.
- During this pandemic, refrain from posting or sharing any information that has not been verified.
- Refrain from installing and investing through suspicious money earning apps offering quick high returns/ benefits.
- Imposters are posing as armed forces personnel to collect fake donation. Hence always verify donation requests before contributing. Report and check suspect on cybercrime.gov.in

Note: Any unusual activity or attack should be reported immediately at incident@cert-in.org.in, cert.ksitm@kerala.gov.in with the relevant details for analysis and taking further appropriate actions.