it Principi di sicurezza informatica

Seguire questi principi di sicurezza informatica può aiutare a ridurre il rischio di minacce informatiche alla rete in cui è installato il sistema.

Tieni aggiornato il tuo telefono e installa gli ultimi aggiornamenti di sicurezza.
Connettiti solo a reti Wi-Fi sicure.
Scarica app solo da Google Play o Apple Store.
Usa tutte le impostazioni di sicurezza del tuo cellulare:
· codici lunghi
· autenticazione a due fattori (2FA)
· riconoscimento facciale
· bloccare app sconosciute
Usa password sicure per telefono e account:
· Non riutilizzare una password da nessun altro account.
· Le password devono essere lunghe 12-16 caratteri. (Una passphrase è la cosa migliore e più facile da ricordare.)
· La password deve essere una combinazione di lettere maiuscole, lettere minuscole, numeri, punteggiatura e simboli.
· Non utilizzare una password con informazioni personali facilmente individuabili o comunemente note. Per esempio, evita di usare la città natale, il tuo animale domestico preferito o la mascotte del liceo.

Disattivazione di un dispositivo

Se rimuovi un dispositivo dal tuo sistema per regalare, rivendere o altrimenti smaltire, prima rimuovi qualsiasi elemento di identificazione personale informazioni dal dispositivo eseguendo un ripristino delle impostazioni di fabbrica. Questo è particolarmente importante quando si tratta di disattivazione di un gateway di sistema. Fare riferimento alle istruzioni del dispositivo specifico per informazioni su come eseguire il ripristino delle impostazioni di fabbrica.

en Cybersecurity principles

Following these cybersecurity principles may help to reduce the risk of cyber threats to the network where your system is installed.

Keep your phone up to date and install the latest security updates.
Only connect to secure Wi-Fi networks.
Only download apps from Google Play or Apple store.
Use all of your mobile phone's security settings:
· long passcodes
· two-factor authentication (2FA)
· facial recognition
· block unknown apps
Use strong phone and account passwords:
· Do not reuse a password from any other account.
· Passwords should be 12-16 characters long. (A passphrase is best and easier to remember.)
· The password must be a combination of uppercase letters, lowercase letters, numbers, punctuation and symbols.
· Do not use a password with easily guessed or commonly known personal information. For example, avoid using home town, favorite pet or high school mascot.

Decommissioning a device

If you remove a device from your system to gift, resell or otherwise dispose of, firstly remove any personallyidentifiable information from the device by performing a factory reset. This is especially important when decommissioning a system gateway. Refer to the particular device instructions for information on how to perform the factory reset.

Schneider Electric

fr Principes de cybersécurité

Le respect de ces principes de cybersécurité peut aider à réduire le risque de cyberattaques sur le réseau où votre système est installé.

Gardez votre téléphone à jour et installez les dernières mises à jour de sécurité.
Connectez-vous uniquement à des réseaux Wi-Fi sécurisés.
Téléchargez uniquement des applications à partir de Google Play ou Apple Store.
Utilisez tous les paramètres de sécurité de votre téléphone mobile:
· longs codes d'accès
· authentification à deux facteurs (2FA)
· reconnaissance faciale
· blocage des applications inconnues
Utilisez des mots de passe forts pour le téléphone et le compte:
· Ne réutilisez pas un mot de passe d'un autre compte.
· Les mots de passe doivent comporter entre 12 et 16 caractères. (Choisir une phrase secrète est la meilleure façon pour la retenir plus facilement).
· Le mot de passe doit être une combinaison de lettres majuscules, minuscules, chiffres, ponctuation et symboles.
· N'utilisez pas de mot de passe contenant des informations personnelles facilement devinables ou connues. Par exemple, évitez d'utiliser la ville natale, l'animal de compagnie préféré ou la mascotte du lycée.

Mise hors service d'un dispositif

Si vous supprimez un dispositif de votre système pour le donner, le revendre ou le déposer, supprimez d'abord toutes les informations personnelles identifiables du dispositif en effectuant une réinitialisation d'usine. Ceci est particulièrement important lors de la mise hors service en cas de système gateway. Reportez-vous aux instructions particulières du dispositif pour obtenir des informations sur la façon d'effectuer la réinitialisation d'usine.

nl Cyberbeveiligingsbeginselen

Door deze cyberbeveiligingsbeginselen in acht te nemen kan het risico beperkt worden gehouden op cyberaanvallen op het netwerk waarop uwsysteem geïnstalleerd is.

Houd uw telefoon up-to-date en installeer de nieuwste beveiligingsupdates.
Maak uitsluitend verbinding met beveiligde Wi-Fi-netwerken.
Download alleen apps van Google Play of Apple store.
Maak gebruik van alle beveiligingsinstellingen van uw mobiele telefoon:
· lange wachtwoorden
· twee-factor-authenticatie (2FA)
· gezichtsherkenning
· onbekende apps blokkeren
Gebruik sterke telefoon- en accountwachtwoorden:
· Gebruik nooit hetzelfde wachtwoord op verschillende accountst.
· Wachtwoorden moeten 12-16 tekens lang zijn. (Een wachtwoordzin is gemakkelijker te onthouden)
· Het wachtwoord moet bestaan uit een combinatie van hoofdletters, kleine letters, cijfers, leestekens en symbolen.
· Gebruik geen wachtwoord die gemakkelijk te raden of algemeen bekende persoonlijke informatie bevat. Bijvoorbeeld, vermijd het gebruik van de woonplaats, favoriete huisdier of middelbare school-mascotte.

Buiten gebruik stellen van een apparaat

Als u een van uw persoonlijke apparaten cadeau wilt geven, verkopen of anderszins wegdoet, verwijder dan eerst al u persoonsgegevens,en traceerbare informatie van het apparaat door het naar fabrieksinstellingen terug te zetten.
Dit is vooral belangrijk om een systeem gateway buiten gebruik te stellen. Raadpleeg de handleiding van het apparaat voor resetinstructies en het naar fabrieksinstellingen terug te zetten

IST004300-Ed.00-07/2021

Schneider Electric Industries SAS
35 Rue Joseph Monier
92500 Rueil Malmaison (France)
Tél : +33 (0)1 41 29 70 00
Fax : +33 (0)1 41 29 71 00
http://www.schneider-electric.com