Cyber Security

Sicherheit und Freiheit ...
... auch im Cyberspace!

Sécurité et liberté ...
... aussi dans le cyberespace !

Sicurezza e libertà ...
... anche nel cyberspazio!

www.cyberdefence.ch

38.010dfi 08.17 10000 SAP 2571.2108

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Schweizer Armee
Armée suisse
Esercito svizzero

	Äusserungen in Sozialen Medien sind immer als öffentlich anzusehen.	Considérez toujours les propos tenus sur les réseaux sociaux comme publics.	Considerate sempre pubbliche le dichiarazioni nei social media.
	Niemals fremde oder private USB-Geräte an Systeme der Armee oder der Verwaltung anschliessen.	Ne jamais connecter un dispositif privé ou inconnu à des appareils de l'administration ou de l'armée.	Mai collegare apparecchi USB sconosciuti o privati a sistemi dell'esercito o dell'amministrazione.
	Öffentliche Hotspots können schädlich sein. Ein Hotspot Ihres eigenen Handys ist sicherer.	Les points d'accès wifi publics peuvent être dangereux. Votre téléphone mobile est un point wifi plus sûr.	Hotspot pubblici possono essere dannosi. Un hotspot con il proprio smartphone è più sicuro.
	WLAN, Bluetooth, GPS, NFC, etc. sind deaktiviert, ausser sie werden bewusst benötigt.	Il faut désactiver WLAN, Bluetooth, GPS, NFC sauf si vous en avez réellement besoin.	WLAN, Bluetooth, GPS, NFC sono disattivati a meno che non siano coscientemente necessari.
	Handys, Uhren und Notebooks sind potenzielle Wanzen. Vor vertraulichen oder geheimen Gesprächen diese Geräte wegschliessen.	Les téléphones portables, montres ou ordinateurs portables sont des mouchards potentiels. Il faut ranger ailleurs ces appareils avant une conversation confidentielle ou secrète.	Cellulari, orologi e notebooks sono potenzialmente delle cimici. Prima di conversazioni confidenziali o segrete riponete altrove questi apparecchi.
	Keine Mitteilungen/Anhänge/Links unerwarteter Herkunft öffnen. Kontaktieren Sie bei Verdacht den Absender telefonisch.	N'ouvrez ni les messages, ni les annexes ou les links de provenance inattendue. Contactez l'expéditeur par téléphone en cas de doute.	Non aprite messaggi/allegati/link di provenienza inattesa. In caso di dubbio contattate il mittente telefonicamente.
	Trennen Sie bei Verdacht auf Malware-Infektion schnellstmöglich die Netzverbindung, lassen Sie das Gerät laufen und melden Sie Ihren Verdacht der Hotline und Ihrem Vorgesetzten.	Si vous soupçonnez une infection par un logiciel malveillant, déconnectez-vous le plus vite possible du réseau, laissez le système en marche et faites part de votre soupçon à la Hotline et à votre supérieur.	In caso si sospetti un'infezione da malware interrompete il prima possibile il collegamento alla rete, lasciate il sistema in funzione e comunicate i vostri sospetti alla hotline e al vostro superiore.