Das 6-Punkte-Programm für bessere Sicherheit in der elektronischen Kommunikation

	Handy/Telefon	PC/Mac	SMS/MMS/E-Mail	WLAN	Allgemein
Dummies	kein Jailbreak Zugangscode definieren Find my iPhone/Lookout installieren Löschen von Apps verhindern	Update - Betriebssystem - Applikationsprogramme Antiviren-Software installieren 2-Way-Firewall verwenden Vorsicht vor problematischen Sites	keine Anhänge unbekannter Absender öffnen	Öffentlichen Zugang unterbinden Komplexe Passwörter verwenden	Passwörter - unterschiedlich pro Website - mind. 6 Zeichen lang, Gross- und Kleinbuchstaben, Ziffern, keine Begriffe aus Wörterbüchern, Namen, keine Geburtstage Nie Rückfragen zu Zugangsdaten oder Passwörtern beantworten Social media: - Datenschutz auf maximal stellen - keine heiklen Infos streuen Kredit-Karten-Infos nur über https-Sites
Normalos	Nie aus der Hand geben! Besseren Zugangscode festlegen Beschränken: - Ortungsfunktion - Internet-Zugang Bei Nicht-Gebrauch abstellen: - Bluetooth - Tethering - WLAN	Boot Password festlegen Epic Browser statt IE, Chrome … Startpage.com statt Google URL eintippen Bei Anmeldung auf selten besuchten Websites falsche persönliche Infos verwenden		Mac-Adressen definieren	Kundenkarten gemeinsam benützen Unaufgefordert zugesandte Newsletters abbestellen Bei Kundenbefragungen Alias-Infos angeben
Business	Backup nur lokal, nicht via Cloud. Cloud-Zugriff der Apps restriktiv definieren Passwort-Manager benützen Keine Apps verwenden, die das Adressbuch oder den Kalender auf externe Server hochladen	PC nicht unbeaufsichtigt herumstehen lassen Nur Cloud-Speicher auf schweizerischen Servern verwenden Plugin TrackerBlock oder Ghostery installieren Regelmässig *alle* Cookies löschen (auch Supercookies) Wegwerf-E-Mail-Adressen lösen	SMS mit End-to-End-Verschlüsselung verwenden	Unterschiedliche E-Mail-Adressen verwenden Den eigenen Namen nicht als Bestandteil der E-Mail-Adresse angeben Wichtige E-Mail-Accounts auf schweizerischen Servern platzieren	Passwörter: mind. 8 Stellen lang Keine privaten Infos "posten" in den social media

	Handy/Telefon	PC/Mac	SMS/MMS/E-Mail	WLAN	Allgemein
Admins	Hülle verwenden, die die Front-Kamera abdeckt Immer mit der Rückseite gegen unten ablegen	Fingerabdruck-Scanner verwenden Beim Weggehen Bildschirm sperren Linse der eingebauten Kamera abdecken Mikrofon-Öffnung abdecken Daten im Cloud-Speicher nur verschlüsselt ablegen VPN-Verbindungen verwenden Passwörter manchmal wechseln	Verschlüsselte E-Mail-*Übertragung* verwenden	Keine fixe IP-Adresse verwenden	Passwörter mind. 10 Stellen lang USB-Sticks sicher verwahren
VIP	Wegschliessen oder abstellen vor vertraulichen Gesprächen	Gehäuse-Verschluss sichern Anschlüsse regelmässig kontrollieren (z.B. auf Hardware Key Logger) Hardware-Token verwenden statt Boot-Passwort Definitive Löschung nicht mehr benötigter Daten Zugriff auf heikle Daten nur über zusätzliche Schranke (z.B. RSA Key) Tor-Netzwerk verwenden mit Onion Browser Nur verschlüsselte Datenspeicher verwenden (Disk, USB-Stick)	*Inhalt* der E-Mails verschlüsseln. Dienste mit PFS (Perfect Forward Secrecy) benützen.		Zertifikate von aufgerufenen https-Sites prüfen
Paranoics	Abhörsicheres Telefon verwenden. Kein normales Handy herumtragen. Professionelle Chiffriergeräte einsetzen	PC/Mac vom Internet abkoppeln; Verbindung zum Internet nur über eine dedizierte Maschine; Kommunikation via USB-Stick. PC/Mac abschirmen. Keine Zusatztastaturen verwenden. USB-Stick regelmässig ersetzen.			Keine elektronischen Geräte übers Internet bestellen. Keine Hotel-Reservationen übers Internet.