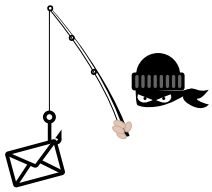
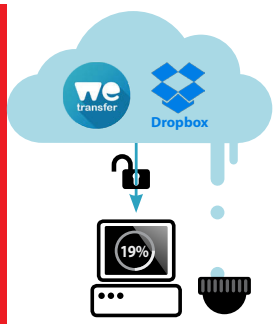
NEDERLANDSE ORDE VAN ADVOCATEN

Tips voor vertrouwelijke internetcommunicatie

Veilig gebruik digitale communicatiemiddelen

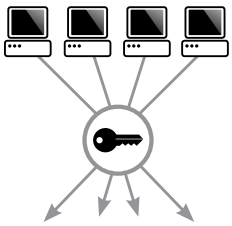
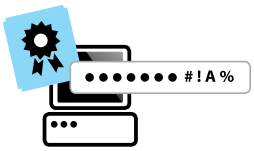
		ADVIES	TOELICHTING
E-MAIL		Alleen geschikt voor algemene communicatie, maar in principe nooit voor uitwisseling van vertrouwelijke informatie.	Uitwisseling van vertrouwelijke informatie alleen indien beide partijen onderling mailverkeer kunnen versleutelen.
TELEFONIE EN SMS		Bel of sms met uw geheimhoudersnummer. Alleen geschikt voor het maken van afspraken, etc. Niet voor het delen van inhoudelijke informatie.	Gebruik voor vertrouwelijke communicatie alleen beveiligde kanalen.
WHATSAPP		Alleen geschikt voor algemene communicatie. Omdat WhatsApp inzicht heeft in alle telefoonnummers en e-mailadressen die u in uw telefoon hebt opgeslagen, is gebruik af te raden als u uw contacten vertrouwelijk wilt houden.	WhatsApp versleutelt tegenwoordig verkeer, maar dit verloopt via Amerikaanse systemen en is niet goed toetsbaar. Absolute veiligheid kan niet worden gegarandeerd. Daarnaast deelt WhatsApp informatie over met wie u appt met Facebook.
DROPBOX, WETRANSFER OF VERGELIJKBARE DIENST		Niet geschikt voor delen van vertrouwelijke documenten. Ga er vanuit dat deze diensten meekijken. Zonder extra voorzorgsmaatregelen is gebruik hiervan zelfs als datalek te kwalificeren!	Alleen gebruiken voor bestanden die u zelf vooraf hebt versleuteld.

FOX IT
FOR A MORE SECURE SOCIETY

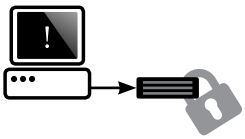
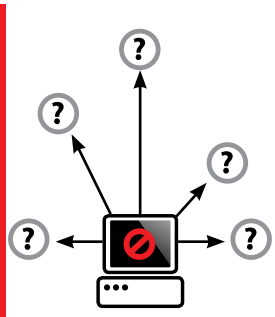
NEDERLANDSE ORDE VAN ADVOCATEN

Tips voor vertrouwelijke internetcommunicatie

Organisatie van uw IT-beheer

		ADVIES
IT-BEHEER		• Gevoelige informatie gaat uitsluitend over versleutelde verbindingen. • Op alle systemen is aandacht voor beveiliging (updates, geen onnodige software, configuratie). • Maak afspraken met de dienstverlener, inclusief over transparantie en reactiesnelheden bij informatiebeveiligingsincidenten. • Maak afspraken over wie de eigenaar van data is, als de dienstverlener wordt overgenomen of failliet gaat.
AUTHENTICATIE MET BETREKKING TOT SYSTEMEN MET GEVOELIGE/ VERTROUWELIJKE INFORMATIE		• Gebruik een sterk wachtwoordbeleid voor individuele persoonlijke accounts (bijvoorbeeld meer dan 14 tekens, geen woordenboek-woorden). • Voeg een tweede factor voor authenticatie toe, zoals Google Authenticator, of gebruik een certificaat (zoals de Advocatenpas).

Diverse eigen systemen

		ADVIES	TOELICHTING
VEILIGHEID VAN WERK-STATIONS EN MOBIELE APPARATEN		• Gebruik een firewall en antivirus-programma's. • Ga risicobewust te werk. • Voer veiligheidsupdates tijdig door.	• Zet gevoelige informatie achter login. • Maak geen gebruik van publieke wifi. • Gebruik zakelijke apparaten niet voor privédoeleinden.
VEILIGHEID VAN BACK-UPS		• Beveilig het opslagsysteem. • Zorg ervoor dat geen onnodige toegang mogelijk is.	• Test ook de back-ups. • Maak afspraken over verantwoording en incidentmanagement.
HOEVEEL DATA DEELT MIJN BESTURINGS-SYSTEEM EN/OF GEBRUIKTE APPLICATIES) MET DERDEN? IS HET GESCHIKT VOOR MIJ?		• Controleer (zoek online of gebruik een diagnostische tool) welke informatie gedeeld wordt. • Loop in het besturingssysteem, webbrowsers en applicaties zelf de instellingen langs. • Kijk of er best practices bestaan. • Kijk goed naar de instellingen voor het delen van contact-gegevens en locaties.	• Beoordeel op basis van de End User License Agreement welke informatie gedeeld kan worden en schat het risico in. • Overweeg het gebruik van ad-blockers (plugins om de browser verder te beveiligen). • Overweeg om alle gevoelige informatie en/of applicaties achter extra authenticatie te zetten.