NEDERLANDSE ORDE VAN ADVOCATEN

TIPS voor vertrouwelijke internetcommunicatie

De menselijke factor: Veruit de meeste inbraken op systemen beginnen doordat iemand op een link klikt in een e-mail of sms (phishing), via de telefoon een wachtwoord of andere informatie afgeeft aan een zogenaamde collega of door in te loggen terwijl iemand anders stiekem meekijkt (social hacking). Veiligheid begint met weten hoe en waar u kwetsbaar bent.

VEILIG GEBRUIK DIGITALE COMMUNICATIEMIDDELEN

CLOUDDIENSTEN VOOR BESTANDSUITWISSELING

Geschikt voor het delen van vertrouwelijke informatie mits de optie tot vergrendeling wordt aangeboden. Verstuur vertrouwelijke bestanden uitsluitend met vergrendeling en na raadpleging van het Privacy & Cookie-Statement van de betreffende clouddienst.

Het is bijna niet uit te sluiten dat derden bij dit soort diensten meekijken.

E-MAIL

Gebruik onbeveiligde e-mail voor algemene communicatie, maar niet voor uitwisseling van vertrouwelijke informatie.

Diverse commerciële e-mailprogramma's bieden de optie om berichten versleuteld te versturen. Let op: de persoon waar u mee mailt moet ook dergelijke maatregelen nemen.

TELEFONIE EN SMS

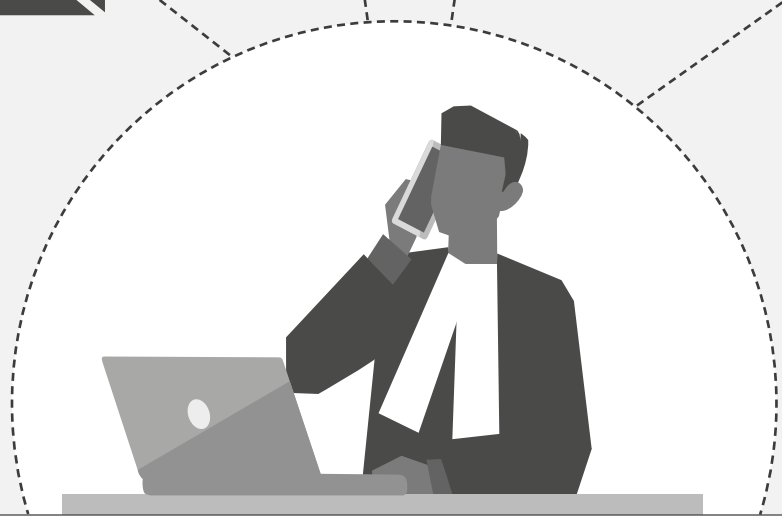
Gebruik altijd uw geheimhoudernummer. Bel of sms niet vertrouwelijk met uw gewone telefoon.

Gebruik uw telefoon voor het maken van afspraken en dergelijke. Niet voor het delen van inhoudelijke informatie.

CHAT-APPS

Gebruik chat-apps voor algemene communicatie. Chat-apps kunnen inzicht hebben in telefoonnummers en e-mailadressen die staan opgeslagen in uw telefoon. Het gebruik is af te raden wanneer u uw contacten vertrouwelijk wilt houden.

Chat-apps versleutelen veelal het dataverkeer. Dit verloopt mogelijk via buitenlandse systemen. Absolute veiligheid kan niet worden gegarandeerd.



ORGANISATIE VAN UW IT BEHEER

IT BEHEER

Leid gevoelige informatie uitsluitend over versleutelde verbindingen.

Geef op alle systemen aandacht aan de beveiliging (security-updates, geen onnodige software, juiste configuratie).

Maak afspraken met uw IT-aanbieder, ook over transparantie en reactiesnelheden bij (informatie) beveiligingsincidenten.

AUTHENTICATIE SYSTEMEN MET GEVOELIGE INFORMATIE

Gebruik alleen persoonlijke accounts en een sterk wachtwoordbeleid.

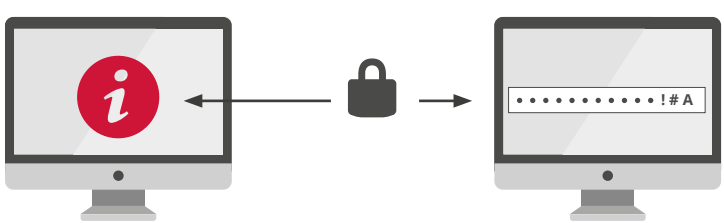
Voeg een tweede factor voor authenticatie toe, of gebruik een certificaat (zoals de advocatenpas).

Gebruik bij voorkeur een wachtwoordkluisje voor beheer van uw wachtwoorden.

AUDIT

Regel de benodigde AVG verwerkersovereenkomsten inclusief een procedure voor datalekken. Weet hoe te reageren op een datalek en deze te rapporteren.

Zorg voor auditlogs over het gebruik en de verzending van vertrouwelijke informatie, voor het geval een datalek of beveiligingsincident optreedt.



DIVERSE EIGEN SYSTEMEN EN DIENSTEN

	Techniek	Organisatie
VEILIGHEID VAN WERKSTATIONS EN MOBIELE APPARATEN	▸ Gebruik een firewall en antivirusprogramma's. ▸ Voer security-updates tijdig door. ▸ Overweeg om alle gevoelige informatie en/of applicaties achter extra authenticatie te zetten.	▸ Ga risicobewust te werk. ▸ Maak **geen** gebruik van publieke wifi. ▸ Gebruik zakelijke apparaten niet voor privé. ▸ Laat periodiek een security-assessment of penetratietest uitvoeren.
VEILIGHEID VAN BACK-UPS	▸ Beveilig het opslagsysteem. ▸ Zorg dat backups elders worden bewaard. ▸ Zorg ervoor dat geen onnodige toegang mogelijk is.	▸ Test de back-ups. ▸ Maak afspraken over verantwoording en incidentmanagement.
WELKE DATA DEELT MIJN APPARAAT MET DERDEN?	▸ Controleer (zoek online of gebruik een diagnostische tool) welke informatie gedeeld wordt. ▸ Loop in het besturingssysteem, de webbrowsers en de applicaties de instellingen na. Veel apps vragen toegang tot bestanden van andere apps of diensten. Beoordeel dat kritisch. ▸ Kijk of er best practices bestaan. ▸ Kijk goed naar de instellingen voor het delen van contactgegevens 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 adblockers (plugins om de browser verder te beveiligen).
GEBRUIK VAN CLOUDDIENSTEN (ZOALS O365)	▸ Vereis dat de toegang tenminste met 2-factor authenticatie plaatsvindt. ▸ Leg vast wie de eigenaar van data is en hoe deze wordt teruggegeven wanneer het contract eindigt en wanneer de dienstverlener wordt overgenomen of failliet gaat.	▸ Onderzoek certificering van dienstverleners. ▸ Bepaal zelf in welk land de data wordt opgeslagen omdat privacyregelgeving per land verschilt. ▸ Wees alert op met wie en wat uw gegevens worden gedeeld door de dienstverlener.
DATA HYGIËNE	▸ Beperk de opslag van gegevens tot de applicaties of diensten waarvoor ze nodig zijn. ▸ Verwijder bestanden wanneer ze niet meer nodig zijn. Exporteer geen informatie uit systemen als dat niet noodzakelijk is.	▸ Deel gevoelige informatie alleen versleuteld en met de mogelijkheid van intrekken. ▸ Beperk toegang tot gevoelige informatie tot need-to-know. ▸ Maak **geen** gebruik van USB-sticks

Voor deze infographic geldt de disclaimer die te vinden is op advocatenorde.nl