NEDERLANDSE ORDE VAN ADVOCATEN

TIPS voor vertrouwelijke internetcommunicatie

Als advocaat werkt u per definitie met vertrouwelijke informatie. Uw gegevens en die van uw cliënten kunnen voor cybercriminelen veel waard zijn. De kans dat u slachtoffer wordt van datadiefstal is bovengemiddeld groot en kan ingrijpende gevolgen hebben. Bent u zich bewust van de risico's? Weet u welke van uw communicatiemiddelen wel of niet veilig zijn? Welke maatregelen u kunt treffen om u tegen een cyberaanval te beschermen? Wat moet u doen bij een datalek? Om u bij de antwoorden op deze vragen op weg te helpen, heeft de NOvA een aantal tips voor vertrouwelijke internetcommunicatie voor advocaten op een rij gezet.

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

VEILIG GEBRUIK DIGITALE COMMUNICATIEMIDDELEN

CLOUDDIENSTEN VOOR BESTANDUITWISSELING

Geschikt voor het delen van vertrouwelijke informatie mits de optie tot vergrendeling wordt aangeboden. Het is bijna niet uit te sluiten dat derden bij dit soort diensten meekijken.

Verstuur vertrouwelijke bestanden uitsluitend met vergrendeling en na raadpleging van het privacystatement van de betreffende clouddienst.

E-MAIL

Onbeveiligde e-mail is geschikt voor algemene communicatie, niet voor uitwisseling van vertrouwelijke informatie.

Diverse commerciële e-mailprogramma's bieden de optie om berichten versleuteld te versturen. Let op: de Rechtspraak stelt specifieke eisen aan veilig mailen.

TELEFONIE EN SMS

Geschikt voor het maken van afspraken en dergelijke, niet voor het delen van inhoudelijke en vertrouwelijke informatie.

Zorg dat uw telefoonnummer bij de NOvA bekend is als geheimhoudernummer. Bel of sms altijd met uw vertrouwelijke geheimhoudernummer en niet met uw privételefoon.

CHAT-APPS

Chat-apps kunnen inzicht hebben in gegevens (telefoonnummers, e-mailadressen, locaties, gespreksmetadata, IP-adres) die staan opgeslagen in uw telefoon. Het gebruik is geschikt voor algemene communicatie, maar af te raden wanneer u uw contacten vertrouwelijk wilt houden.

Chat-apps versleutelen veelal het dataverkeer, maar absolute veiligheid kan niet worden gegarandeerd. Kies voor een privacyvriendelijke chat-app.

IT-BEHEER

INRICHTING IT-OMGEVING

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 beveiligingsincidenten.

AUTHENTICATIE

Gebruik alleen persoonlijke accounts en een sterk wachtwoordbeleid.

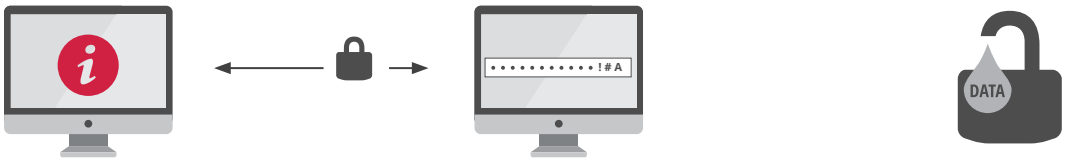
Voeg een tweede factor voor authenticatie toe of gebruik een certificaat (zoals de advocatenpas).

Gebruik bij voorkeur een wachtwoordkluisje voor beheer van uw wachtwoorden.

AVG EN AUDIT

Regel de benodigde AVG-verwerkersovereenkomsten inclusief een procedure voor datalekken.

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



SYSTEMEN EN DIENSTEN

	Techniek	Organisatie
VEILIGHEID VAN WERKSTATIONS EN MOBIELE APPARATEN	▸ Gebruik een firewall en antivirusprogramma's. ▸ Voer securityupdates door. ▸ Plaats alle gevoelige informatie en/of applicaties achter een extra authenticatie.	▸ Ga risicobewust te werk. ▸ Maak geen gebruik van publieke wifi. ▸ Gebruik zakelijke apparaten niet voor privédoeleinden. ▸ Laat periodiek een security-assessment of penetratietest uitvoeren.
VEILIGHEID VAN BACK-UPS	▸ Beveilig het opslagsysteem. ▸ Zorg dat back-ups (ook in de cloud) 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?	▸ 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/locaties en toegang tot camera/microfoon.	▸ Beoordeel op basis van de gebruikersovereenkomst welke informatie gedeeld kan worden en schat het risico in. ▸ Overweeg het gebruik van adblockers (plug-ins om de browser verder te beveiligen).
GEBRUIK VAN CLOUD-DIENSTEN (ZOALS O365)	▸ Vereis dat de toegang tenminste met 2-factorauthenticatie 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 privacywetgeving per land verschilt. ▸ Wees er alert op met wie en wat uw gegevens worden gedeeld door de dienstverlener.
DATAHYGIËNE	▸ 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 onbeveiligde USB-sticks.
E-SIGNING	▸ Kies een methode voor e-signing die toekomstvast is. ▸ Onderzoek of de elektronische handtekening onafhankelijk van de leverancier kan worden gevalideerd. ▸ Zorg voor een afzonderlijk bewijs van ondertekening los van het ondertekende document (audit trail).	▸ Bepaal welke type elektronische handtekening toereikend is voor uw verschillende soorten documenten. ▸ Ga na of de door u gekozen methode voor e-signing rechtsgeldig is (voldoet aan de juiste standaarden).

Versie juli 2022

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