DEFENSIE
Uw toekomst. Onze missie.

Richtlijnen voor een goed gebruik

van de sociale media

.be

De sociale media maken deel uit van ons dagelijkse leven we wisselen er info uit, zoeken er info, plaatsen er berichten...

Als militair gebruiken we ze om contact te houden met onze naasten als we in operatie zijn.

Onze families posten informatie over ons gezinsleven dat overhoop gegooid wordt door het vertrek op operatie of delen hun interesse in onze activiteiten.

We vullen onze loopbaan bij Defensie in op onze persoonlijke pagina's.

Ons beroep is immers een belangrijk deel van ons dagelijks leven. En we delen dat graag met onze omgeving.

Maar zijn al deze handelingen wel volledig veilig?

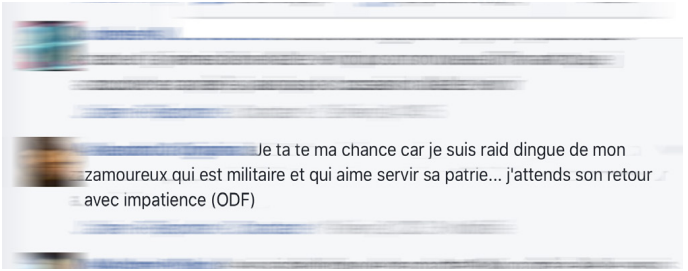
Welke risico's lopen we als we deze informatie delen?

In welke mate kunnen ze tegen ons worden gebruikt?

Voorbeelden

Wijzelf of onze omgeving posten soms info die ons verraadt: informatie over onze opdracht, een voorval met impact op onze operationele capaciteiten, de voorbereiding, de samenstelling van een konvooi dat op het punt staat te vertrekken…

Two belgian army armoured vehicle MPPV Dingo 2 overturns on side in Afghanistan Defense News



Algemeen

Informatie die op het internet gepubliceerd wordt, is nooit onschuldig of vertrouwelijk.

In moderne conflicten scannen onze «vijanden» regelmatig het web (sociale netwerken, blogs, forums, persoonlijke websites…) op zoek naar gevoelige informatie alsook om de zwakheden van Defensie op te sporen.

Dit constant verzamelen van gegevens kan u, uw omgeving en ook Defensie rechtstreeks schade berokkenen.
Als medewerker bij Defensie moet u dus uiterst waakzaam zijn.

In deze brochure geven we u 4 aanbevelingen om te vermijden dat u informatie vrijgeeft die tegen u zou kunnen worden gebruikt. Het gaat om de veiligheid van Defensie, om uw eigen veiligheid, maar ook om die van uw familie.

Aanbeveling 1
Ik let op wat ik post

Ik publiceer geen geclassificeerde informatie over een lopende of geplande operatie: datums, plaatsen en uren van patrouilles, aard van de opdrachten, doelen…
In operatie publiceer ik nooit content met op de achtergrond een gebouw, geclassificeerd materiaal of eender welke informatie waarmee mijn eenheid geïdentificeerd kan worden (badge, naamlint, kaart, locatie…).
Ik tag de namen van mijn collega's **niet** op mijn content.
Ik blijf discreet over mijn functie, ik geef niet te veel details over mijn opdrachten op de professionele netwerken.

Ik denk eraan dat elke informatie die ik publiceer over mijn functie en mijn activiteiten bij Defensie tegen mij en/of mijn familie gebruikt kan worden en het goede verloop van een operatie in gevaar kan brengen.

Mensen zien me altijd als een werknemer van Defensie, ook in mijn vrije tijd.
In ieder bericht of commentaar respecteer ik de waarden van Defensie: integriteit en loyauteit.
Ik onthoud me van ieder gedrag dat schadelijk is voor het imago van Defensie.

Aanbeveling 2

Ik controleer mijn privacyinstellingen

In operatie deactiveer ik de geolokalisatiefunctie van mijn applicaties en schakel de gps van mijn smartphone uit, als die niet noodzakelijk is voor de uitvoering van mijn opdracht.

Ik beperk de toegang tot mijn profiel tot personen die ik persoonlijk ken.

Ik let op wat ik openbaar publiceer.

Ik deactiveer de automatische tagging zodat ik niet op content geïdentificeerd kan worden zonder dat ik het weet.

Goed communiceren op sociale media betekent ook dat u de privacyinstellingen kent en vermijdt dat er informatie gepubliceerd wordt zonder dat u het weet.

Aanbeveling 3
Ik spreek erover met mijn omgeving

Ik maak mijn familie en vrienden bewust van de mogelijke risico's.

Ik vraag hun om deze regels te respecteren, vooral wanneer het gaat om plaatsen waar ik ben, datums van terugkeer en van manoeuvres…

Hoe meer de mensen uit mijn omgeving informatie over mijn activiteiten bij Defensie online publiceren, des te meer ze onbewust gegevens openbaar maken die tegen mij of tegen hen kunnen worden gebruikt!

Aanbeveling 4
Ik denk aan de cyberveiligheid

Ik bescherm mijn computer en de ermee verbonden apparaten en ik zorg ervoor dat cybercriminelen geen toegang kunnen krijgen.

Zijn mijn wachtwoorden veilig? Ben ik beschermd tegen virussen?

Kan men in mijn computersysteem binnendringen?

Ik test de bescherming van mijn apparaten op safeonweb.be en ik volg de aanbevelingen.

Algemene aanbevelingen

Vooraleer iets te publiceren, denk eraan dat uw bestemmelingen misschien niet allemaal goede bedoelingen hebben.
De vrienden van uw vrienden zijn niet noodzakelijk uw vrienden.
Als personeelslid van Defensie kan een gebrek aan terughoudendheid bij het delen van uw meningen, van uw politieke, filosofische of geloofsovertuigingen of een gebrek aan respect tegenover Defensie zich snel tegen u keren.
Gebruik altijd uw gezond verstand en denk goed na voor u informatie deelt via de sociale media.
Zelfs zonder uniform blijft u altijd militair.
Laat u niet blindelings verleiden door de nieuwe functies (live streaming, Snapchat) en pas altijd de voorzorgsbeginselen op deze nieuwe technologieën toe.

Er verschijnen regelmatig nieuwe technologieën en applicaties en ik blijf dezelfde beginselen toepassen.

Houd er rekening mee dat bepaalde diensten die de sociale media aanbieden (mailing, VoIP…) niet dezelfde veiligheid bieden als de diensten die Defensie aanbiedt. Het is dus sterk aangeraden om deze niet voor professionele con¬tacten te gebruiken.
Dankzij de nieuwe technologieën hebben we nu ook met internet verbonden apparaten. Op bepaalde gebieden bieden ze een echte meerwaarde. Denk eraan dat deze technologieën heel wat meer informatie verzamelen dan wij vermoeden. En dat deze informatie zonder toestemming via de sociale media kan worden gedeeld.
Ik pas dezelfde voorzorgsmaatregelen toe in mijn digitale leven als in mijn openbare leven.
Ik informeer me goed over de bestaande wetgeving, reglementen en directieven met betrekking tot vrije meningsuiting en respecteer deze bij al mijn activiteiten op de online media

Communicatie van de eenheden

Ik communiceer niet uit eigen beweging in naam van mijn eenheid of Defensie. Enkel de woordvoerder, de persdienst van Defensie of zijn afgevaardigden zijn daartoe bevoegd.

Wanneer een eenheid via de sociale media wenst te communiceren, moet zij vooraf het contactpunt voor communicatie (DELCOM) hiervan op de hoogte brengen en doorgeven wie de verantwoordelijke uitgever is (de korpscommandant).
De berichten handelen enkel over onderwerpen op het niveau eenheid en haar activiteiten. Hierbij wordt altijd de nodige aandacht besteed aan het goede imago en de reputatie van Defensie en worden de regels met betrekking tot de operationele veiligheid nauwgezet gevolgd.
De verantwoordelijke uitgever zorgt ervoor dat alle richtlijnen, reglementen en wetten over communicatieactiviteiten nageleefd worden. Maar hij moet ook zorgen voor de nodige capaciteiten (de steun is meestal gratis, maar een dergelijke activiteit vraagt ook veel tijd, middelen en personeel).

Raad nodig? DG StratCom kan te allen tijde geraadpleegd worden.
Wanneer mogelijk is het sterk aangeraden om een charter te gebruiken.

Voorstel van een charter voor de gebruikers:

Deze pagina is de officiële pagina van <naam van de instelling>. Berichten en informatie die door de internetgebruikers gedeeld en/of uitgewisseld worden, geven hun persoonlijke opvattingen weer en niet het officiële standpunt van <naam van de instelling>.
Wij vestigen uw aandacht op het respect voor de persoonlijke levenssfeer en de wetgeving inzake auteursrechten.
We behouden ons het recht voor om berichten te verwijderen waarvan de inhoud een volgend karakter heeft:
• aanstootgevend, lasterlijk, beledigend of grof;
• racistisch, xenofoob, revisionistisch of negationistisch;
• discriminerend op basis van geslacht of seksuele geaardheid, religie, etnische afkomst;
• pornografisch of obsceen;
• reclame, commercieel karakter of sponsoring behalve voor overeenkomsten tussen <naam van de instelling> en derde partijen;
• beledigend voor de instelling en/of de personen die er werken.

Als deze regels niet worden nageleefd, dan kan de gebruiker van deze pagina worden uitgesloten.

Contactpunten

Als u een incident vaststelt dat de veiligheid van Defensie of van haar personeel kan schaden, neem dan contact op met de veiligheidsofficier van uw eenheid.

Als u het slachtoffer bent van kwaad opzet (identiteitsdiefstal, hacken van uw gegevens…), neem dan contact op met de computer crime unit van de federale politie via de website: https://www.ecops.be/ en meld dit aan uw veiligheidsofficier.

In geval van pesterijen: contacteer de vertrouwenspersoon van uw eenheid.

Voor meer informatie: http://infosec.mil.intra