SECURITE ¦ ATTENTION

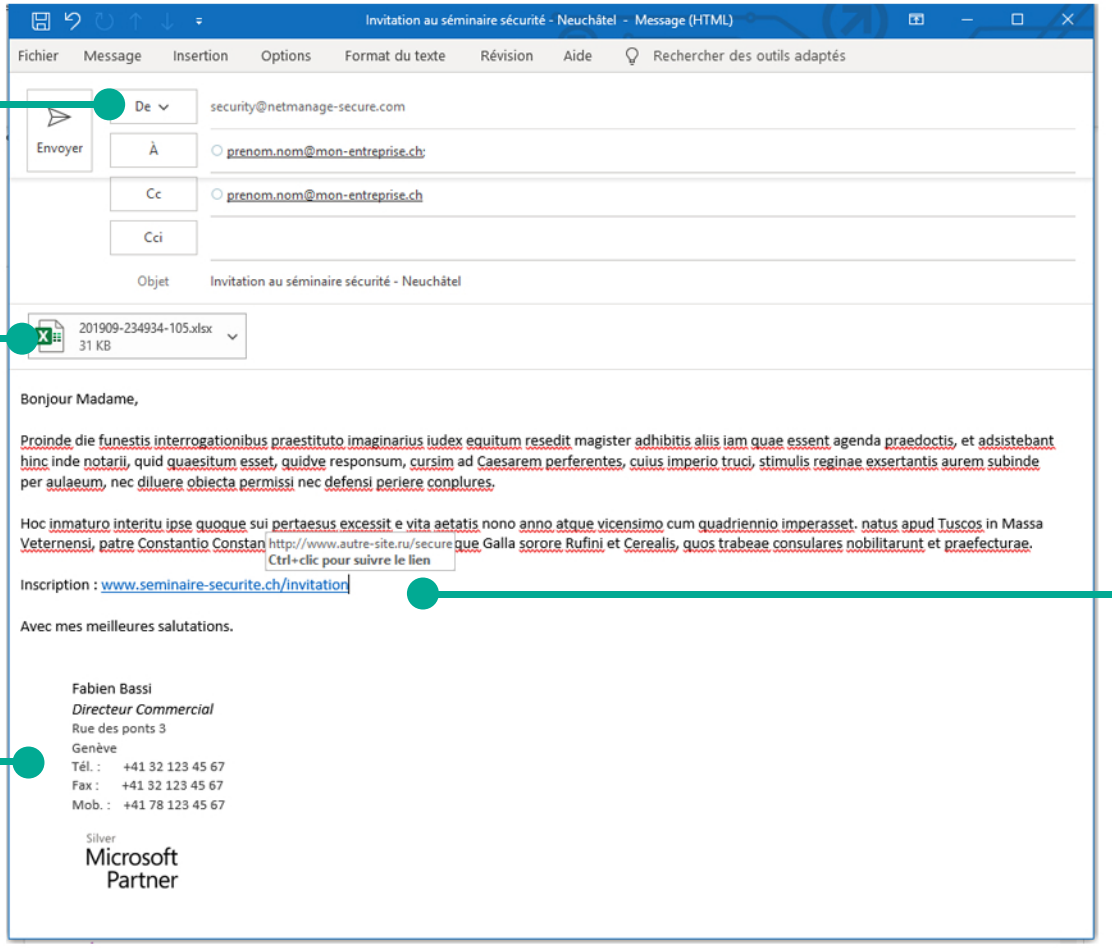
LES COURRIERS ÉLECTRONIQUES

Les courriels et leurs pièces jointes ont un rôle central dans la propagation d'attaques cyber.
Lorsque vous recevez des courriers électroniques, soyez vigilant à l'ensemble des indicateurs ci-dessous :

Assurez-vous de la véracité de l'émetteur en lisant son adresse e-mail lettre par lettre. Ne vous fiez pas aux Nom et Prénom qui s'affichent.
Attention au faux domaine, après le @ le domaine peut-être un domaine «fake».
Par exemple: Au lieu de @netmanage.ch -> @netmanage-secure.com
Vérifier toujours le domaine de l'expéditeur.

N'ouvrez jamais une pièce jointe si vous avez le moindre doute

Vérifier la signature de l'expéditeur. Les adresses et numéros si nécessaire



Ne cliquez jamais sur un lien si l'e-mail provient d'une personne que vous ne connaissez pas Il peut arriver que le lien qui s'affiche dans l'e-mail recèle un autre lien. Avant de cliquez, passez simplement la souri au dessus du lien et vérifiez le contenu !

Demande de modification de mot de passe ?
Demande de renseignements bancaires ?
Demande de paiement ?
Demande urgente ?
Méfiez-vous !

Suspicion d'usurpation d'identité ?
Fiez-vous à votre intuition :
contactez la personne concernée ou votre service informatique préférablement par téléphone

Mots de passe

Choisissez vos mots de passe soigneusement et gardez-les confidentiels
Optez pour un mot de passe de 10 caractères minimum comprenant une majuscule, un chiffre et un caractère spécial (€, #...).
Méfiez-vous de toute demande de modification de mot de passe non sollicitée par vous-même.
Modifiez vos mots de passe régulièrement.
Evitez d'utiliser le même mot de passe pour plusieurs plateformes ou applications.

Conseils sécurité

os données professionnelles ne doivent pas être stockées sur des équipements personnels (clé USB, téléphone, cloud, ...).
Sauvegardez vos données professionnelles sur votre espace de stockage en ligne dédié ou sur un équipement testé et fourni par votre entreprise
Sur les réseaux sociaux, n'en dites pas trop à propos de vous ! Les hackers se servent de ces informations pour faire de l'ingénierie sociale : ils se renseignent sur vous, votre localisation, votre poste... et créent des scénarii pour vous piéger ou piéger votre entreprise/entourage.