

PLAN DE COURS

FORMATION : CYBERSECURITE : FACTEUR HUMAIN, MEILLEURE LIGNE DE DEFENSE



LES EXPERTS EN DÉVELOPPEMENT

LE GROUPE MP-PLUS OFFRE DES FORMATIONS PERSONNALISÉES EN ENTREPRISE DEPUIS PLUS DE 25 ANS. PLUS 3500 PARTICIPANTS SUIVENT NOS FORMATIONS ANNUELLEMENT.

NOS FORMATIONS SONT PRISÉES, CAR ELLES SONT FORMATÉES & PERSONNALISÉES POUR CHACUNE DES ENTREPRISES AVEC QUI NOUS COLLABORONS.

À PROPOS DU GROUPE MP-PLUS

Le Groupe MP-Plus est un chef de file dans le domaine de la formation et du développement des professionnels, dont la vision consiste à faire du Québec une référence mondiale en matière de leadership, d'accomplissement et de plaisir au travail. D'ailleurs, notre mission est « Contribuer à l'essor des professionnels en optimisant leur potentiel humain ».

Notre marque de commerce est certes l'impact que nos formations produisent sur les résultats des organisations, et ce, à tout coup. Notre engagement total, notre expertise et nos processus très rigoureux nous permettent d'y arriver.

Depuis plus de 30 ans, Groupe MP-Plus a formé et mobilisé le personnel de grandes corporations ayant eu un impact direct sur plus de 250 000 personnes.

À titre de consultant externe, le Groupe MP-Plus a encadré le virage client entrepris par le Mouvement Desjardins et a aidé plusieurs des 100 plus grandes entreprises au Québec à connaître une croissance fulgurante.

Groupe MP-Plus doit sa réputation à la qualité exceptionnelle de ses interventions et de ses formateurs. Elle compte notamment dans son équipe des sommités comme, Sylvain Guimond, docteur en psychologie du sport et chroniqueur à RDS Christian Martineau, figure réputée dans le domaine du langage non verbal en affaires, et anciennement Mme Monique Jérôme-Forget, ex-vice-première ministre du Québec.

Chaque formation MP-Plus est un pas de plus vers la meilleure version de votre organisation.



François Trachy, Directeur du développement



FORMATION - Cybersécurité : Facteur humain, meilleure ligne de défense

Durée : 4 heures

Contexte

À l'ère du télétravail, de la mobilité et de l'hyperconnexion, la majorité des incidents de cybersécurité ne proviennent plus de failles technologiques, mais bien d'erreurs humaines. Courriels frauduleux, appels trompeurs, deepfakes ou manipulations sociales exploitent nos réflexes, notre confiance et parfois notre urgence d'agir. Cette formation vise à outiller concrètement les participants afin qu'ils comprennent les menaces actuelles, reconnaissent les tactiques des cybercriminels et adoptent des comportements sécuritaires au quotidien. En développant un langage commun et des réflexes clairs, chaque participant devient un acteur clé de la protection de l'organisation. Investir dans le facteur humain, c'est réduire significativement les risques, renforcer la résilience collective et transformer la vigilance individuelle en ligne de défense.

Plan de la formation

Comprendre les fondamentaux et l'enjeu humain :

- **Introduction et mise en contexte**
 - ✓ Accueil et objectifs : Pourquoi l'humain est le « meilleur bouclier »
 - ✓ Sondage interactif sur les habitudes internet et l'auto-évaluation des pratiques cyber
 - ✓ Le risque interne, les incidents et les enjeux humain
- **S'initier au vocabulaire de la cybersécurité pour tous**
 - ✓ Terminologie essentielle (hameçonnage, rançongiciel, etc.)
 - ✓ Introduction aux menaces émergentes
 - ✓ Activité : Démystifier le jargon.
- **Panorama des types d'arnaques spécifiques**
 - ✓ Les bases de la sécurité pour comprendre les concepts fondamentaux pour une vigilance adaptée
 - ✓ Comment repérer l'intention malveillante par les comportements et la communication
 - ✓ Exercice : Analyse d'exemples de courriels ou messages (réels ou simulés) pour déceler les incohérences.

FORMATION - Cybersécurité : Facteur humain, meilleure ligne de défense

Décrypter les tactiques des cybercriminels

- ✓ L'ingénierie sociale : Maîtriser l'art de la manipulation
- ✓ Le Vishing (Vocal Phishing) : Manipulation téléphonique et le « pouvoir de la voix »
- ✓ La menace du Deepfake : Reconnaître les faux contenus audio/vidéo
- ✓ Les visites inattendues/faux inspecteurs : Comment réagir face à la manipulation physique
- ✓ Exercice analyse vidéo

Sécuriser votre environnement numérique au quotidien

- ✓ Protéger votre identité et vos accès
- ✓ Naviguer et communiquer en confiance
- ✓ Exercice d'auto-évaluation

Agir en cas d'incident et développer l'instinct

- ✓ Premiers réflexes en cas d'attaque
- ✓ Signaler la fraude
- ✓ Le pouvoir de l'instinct

Méthodologie pédagogique :

- ✓ Présentations interactives
- ✓ Démonstrations
- ✓ Activités pratiques
- ✓ Échanges et questions-réponses
- ✓ Ressources complémentaires
- ✓ Cahier du participant remis au début de la formation

Matériel nécessaire pour les participants :

- ✓ Connexion internet
- ✓ Ordinateur
- ✓ Accès à la plateforme de visioconférence

Christine Gagnon

Formatrice, conférencière, auteur

Christine Gagnon œuvre dans le domaine de la formation et de l'enseignement universitaire depuis plus de 20 ans. Spécialiste de la communication, de la psychologie appliquée et du comportement humain, elle est aujourd'hui reconnue pour son expertise sur les facteurs humains en cybersécurité, notamment en lien avec le cybercrime, l'ingénierie sociale et les comportements à risque en milieu organisationnel.



Passionnée par le langage, les relations humaines et le développement professionnel, Christine a écrit plusieurs ouvrages de référence en communication utilisé dans divers contextes de formation et d'intervention. Cette solide base lui permet d'aborder la cybersécurité sous un angle stratégique, en mettant l'accent sur la compréhension des comportements, tant du côté des organisations que de celui des cybercriminels.

Au fil des années, elle a bâti une carrière d'enseignante et de formatrice riche et diversifiée. Elle est enseignante invitée à Polytechnique de Montréal, où elle intervient notamment dans les cours Profilage cyber criminel : psychologie du cybercrime et Profilage cyber : comportements et profils de personnalité de cybercriminels. Elle enseigne également à Polytechnique de Montréal auprès de chercheurs, d'enseignants et d'ingénieurs, ainsi qu'à l'Université du Québec à Montréal (UQAM), principalement sur les enjeux de leadership et d'analyse en contexte complexe.

Christine cumule plus de 12 000 heures de formation dispensées auprès d'organisations de premier plan, incluant la Défense nationale, les Forces armées canadiennes, des institutions universitaires et de nombreuses entreprises privées. Elle a livré plus de 650 conférences et formations à travers le Canada et accompagne chaque année des centaines de professionnels et de gestionnaires. Reconnue pour sa capacité à vulgariser des enjeux complexes et à provoquer des changements durables, elle aide les organisations à renforcer leur posture de cybersécurité en misant sur la conscience, la culture et le leadership. Champs de spécialisation :

- Communication relationnelle et cybersécurité
- Profilage cyber criminel et analyse comportementale
- Sémantique linguistique et manipulation
- Gestion de crise et interventions psychologiques
- Leadership et gestion des employés