CYBERSÉCURITÉ : LES BONS RÉFLEXES EN ENTREPRISE

Contenu détaillé

COMPRENDRE LES RISQUES NUMÉRIQUES

- Comprendre les enjeux de la cybersécurité pour le salarié et l'entreprise
- Identifier les principales menaces : phishing, logiciels malveillants, rançongiciels et vol de comptes
- Mesurer les conséquences : perte de données, divulgation d'informations et interruption d'activité
- Connaître son rôle, la charte informatique et les interlocuteurs à contacter

DÉTECTER LE PHISHING ET LES DEMANDES FRAUDULEUSES

- Reconnaître les tentatives de fraude par courriel, SMS, téléphone et QR code
- Repérer les signaux d'alerte : urgence, pression, demande inhabituelle ou changement de coordonnées bancaires
- Vérifier l'adresse de l'expéditeur, le domaine d'un lien et la cohérence du message
- Comprendre qu'un message bien rédigé ou un site en HTTPS peut être frauduleux
- Vérifier une demande sensible par un canal connu, sans utiliser les coordonnées du message suspect
- Adopter les bons réflexes avant d'ouvrir une pièce jointe et ne pas activer de macros sur demande suspecte
- Mise en situation : analyser des messages fictifs et justifier la décision de vérifier ou de signaler

SÉCURISER LES MOTS DE PASSE ET LES ACCÈS

- Créer des mots de passe longs, uniques et difficiles à deviner, selon les règles de l'entreprise
- Découvrir l'authentification multifacteur (MFA) et ses principaux modes de validation
- Refuser une demande de validation inattendue et ne jamais communiquer ses codes de connexion
- Protéger les moyens de récupération et signaler rapidement un compte potentiellement compromis
- Démonstration : générer un mot de passe et utiliser une MFA sur un compte de test

mis à jour le 20.10.2026

CYBERSÉCURITÉ : LES BONS RÉFLEXES EN ENTREPRISE

PROTÉGER LES DONNÉES ET LES SAUVEGARDES

- Distinguer les données personnelles, professionnelles et confidentielles
- Utiliser les espaces de stockage et les outils de partage autorisés par l'entreprise
- Comprendre la différence entre synchronisation et sauvegarde, ainsi que les limites de chacune
- Identifier les fichiers couverts par les sauvegardes et le circuit de demande de restauration
- Comprendre l'intérêt de sauvegardes régulières, protégées et de restaurations testées par le responsable
- Activité : choisir un mode de stockage et de partage adapté à un document

SÉCURISER LE POSTE DE TRAVAIL ET LES SUPPORTS USB

- Verrouiller son écran dès que l'on s'absente et protéger ses équipements contre le vol
- Comprendre le rôle des mises à jour, de l'antivirus et des protections installées
- Installer uniquement les applications et extensions autorisées, sans désactiver les protections
- Ne pas brancher une clé USB inconnue et suivre les règles internes pour les supports amovibles
- Éviter les transferts de fichiers professionnels sur des équipements ou supports personnels non autorisés

UTILISER L'IA EN PRÉSERVANT LA CONFIDENTIALITÉ

- Identifier les risques liés aux prompts, aux fichiers téléversés et aux outils connectés à une IA
- Repérer les informations à ne pas transmettre à ChatGPT ou à un autre service non autorisé : mots de passe, données clients, contrats et documents internes sensibles
- Utiliser les outils et comptes validés par l'entreprise et respecter les usages autorisés
- Préparer une demande avec des données fictives ou réellement anonymisées et vérifier les réponses obtenues
- Activité : tanonymiser des prompts sensibles

mis à jour le 20.10.2026

CYBERSÉCURITÉ : LES BONS RÉFLEXES EN ENTREPRISE

ADOPTER LES BONS RÉFLEXES EN TÉLÉTRAVAIL

- Utiliser les équipements et les accès distants autorisés, avec le VPN de l'entreprise si prévu
- Protéger son réseau domestique et éviter les connexions Wi-Fi publiques non maîtrisées
- Préserver la confidentialité des écrans, des conversations et des documents hors des locaux

RÉAGIR À UN INCIDENT

- Reconnaître les situations à signaler : clic suspect, identifiants divulgués, MFA inattendue ou fichier envoyé au mauvais destinataire
- Interrompre l'action à risque et prévenir rapidement le service informatique ou le référent désigné
- En cas de suspicion d'infection, isoler le poste du réseau selon la procédure interne, sans effacer les traces ni tenter une réparation improvisée
- Transmettre les éléments utiles : heure, message, action effectuée et symptômes constatés
- Mise en situation finale : décrire les premières actions après un clic sur un lien frauduleux

mis à jour le 20.10.2026