arinfo

FORMATION
CYBER SÉCURITÉ

INFORMATIQUE

PROGRAMME COMPLET DE LA FORMATION
1 NIVEAU DISPONIBLE

☆ Opérationnel

MATINÉE *(THÉORIE)* | COMPRENDRE L'ADVERSAIRE

☆ Introduction – «Pourquoi moi ?»

Comprendre pourquoi les petites entreprises sont des cibles privilégiées.
Chiffres clés : le coût d'une cyberattaque pour une petite structure (pertes financières, interruption d'activité, atteinte à la réputation).

☆ Les arnaques du quotidien – Reconnaître les pièges

Savoir en moins de 10 secondes si un email ou SMS est frauduleux.
Le rançongiciel (ransomware) : Comprendre la menace du "kidnapping de données" et les moyens concrets de s'en protéger.

☆ Démasquer les nouvelles fraudes par IA

Comment l'intelligence artificielle rend les arnaques plus crédibles (voix clonées, emails sans faute).
Le réflexe simple qui permet de garder l'avantage face aux arnaques assistées par IA.

☆ Votre caisse à outils – Les 5 réflexes qui sauvent

La méthode simple pour créer des mots de passe forts et uniques.
La double authentification (2FA) expliquée simplement : votre «cadenas numérique».
Mises à jour et sauvegardes : votre assurance-vie numérique.

☆ Plan d'urgence

Les 3 étapes à suivre en cas d'attaque.
Alerter, isoler, redémarrer en sécurité.

☆ Notre retour d'expérience

Comment nous sécurisons nos réseaux intranet et protégeons nos collaborateurs à moindre coût.
Exemples concrets d'outils simples, efficaces et souvent gratuits.
Les erreurs les plus fréquentes observées en entrepries et comment les éviter.

OBJECTIFS

☆ Détecter et neutraliser les tentatives de hameçonnage (phishing) par email et SMS.

Sécuriser les transactions financières de l'entreprise en identifiant les fraudes aux virements (fausse facture, arnaque au président).

Maîtriser la création et la gestion de mots de passe robustes à l'aide d'outils dédiés.

Anticiper les nouvelles menaces utilisant l'Intelligence Artificielle (deepfakes audio, faux documents).

Réagir efficacement en cas d'incident de sécurité en appliquant un protocole d'urgence pour contenir les dégâts.

PRÉ-REQUIS

☆ Aucun prérequis technique n'est nécessaire.

MODALITÉS

PUBLIC

Toutes personnes souhaitant renforcer sa sécurité numérique au travail ou dans sa vie personnelle.

ÉVALUATION

En cours de formation : suivi des acquis.

Fin de formation : questionnaire de satisfaction et attestation de fin de formation.

PÉDAGOGIE

Formation en présentiel, distanciel, ou hybride.

Pédagogie active **« learning by doing »** : la pratique au cœur de la formation à plus de 80%.

Formateur spécialisé dédié et référent pédagogique pour le suivi individuel de la formation.

Assiduité vérifiée par demi-journée avec émargement.

Autre modalité disponible : formation sur mesure, afin de personnaliser le contenu de votre parcours et sa durée pour vous concentrer sur l'essentiel.

Organisme de formation professionnelle spécialisé en Architecture, Graphisme, Design, Web.
N° SIREN : 412 730 269 - N° Activité : 52 44 02924 44 (préfecture de Nantes) - SAS au capital de 466 193,00€ - RCS Nantes B412730269 - Code APE 8559A

APRÈS-MIDI *(PRATIQUE)* | METTRE EN PLACE SA DÉFENSE

☆ Atelier 1 : Chasse au phishing

Objectif concret : appliquer la grille d'analyse apprise le matin pour évaluer rapidement des emails et SMS.
Format : travail en petits groupes ou en binôme
Déroulé : analyse de 5 emails/SMS en binômes + correction collective

☆ Atelier 2 : Simulation d'arnaque téléphonique

Objectif concret : expérimenter la pression d'une tentative d'arnaque au président pour y résister plus efficacement.
Format : jeu de rôle en grand groupe.
Déroulé : jeu de rôle «arnaque au président» avec debrief sur les réflexes anti-manipulation

☆ Atelier 3 : Mains sur le Clavier » – Sécurisation Express

Objectif concret : repartir avec au moins une action de sécurité concrète réalisée sur son propre compte.
Format : travail individuel, accompagné. IMPORTANT : Inviter les participants à venir avec leur smartphone et, si possible, leur ordinateur portable.
Déroulé : chaque participant choisit et réalise 1 action concrète

☆ Atelier 4 : Gestion de crise

Objectif concret : répéter le plan d'urgence dans un timing serré pour ancrer les réflexes.
Format : exercice en groupe entier, chronométré.
Déroulé : synthèse des actions prioritaires à coût nul pour sécuriser réseaux et collaborateurs.

Autre modalité disponible : formation sur mesure, afin de personnaliser le contenu de votre parcours et sa durée pour vous concentrer sur l'essentiel.