

Protéger ses pratiques numériques

Les 21 et 22 mars 2023, soit 14 heures de formation

Nos formations en présentiel se déroulent dans le respect des gestes barrières et d'un protocole sanitaire mis en place pour la protection de tou·tes (mis à jour en fonction de l'évolution de la situation).

➔ Pourquoi cette formation ?

Cette formation propose des méthodes et outils pour penser la sécurisation de ses pratiques, notamment informatiques, comme un processus. Elle permet d'évaluer les outils numériques utilisés ou envisagés au regard de la nature des activités, des menaces existantes, des informations et des correspondant·es que vous cherchez à protéger.

➔ À qui s'adresse cette formation ?

La formation est ouverte à toute personne soucieuse d'améliorer la protection de ses pratiques numérique. Elle s'adresse en particulier aux acteur·rices du milieu associatif souhaitant adopter de bonnes pratiques en matière d'autodéfense numérique et accompagner ces évolutions dans leurs organisations.

➔ Témoignages et taux de satisfaction

Lors de la dernière session de formation, en janvier 2022, les personnes ayant répondu au questionnaire de satisfaction (7 personnes sur les 8 participant·es) étaient globalement très satisfait·es (5 réponses sur 7) ou satisfait·es de leur

formation. Iels ont découvert à quel point « l'aspect juridique est vraiment un plus au sein de la formation, ce qui permet de raccrocher facilement aux préoccupations militantes. ».

Parmi les expressions employées par les participant-es pour décrire la formation, citons : « La sécurité informatique est un processus, pas un produit ! » et « Toustes surveillé-es, sécurisons nos pratiques pour changer le monde ! ».

➔ Objectifs spécifiques de la formation

1. Savoir mettre en place un modèle des risques et des menaces liées à nos pratiques informationnelles – principalement numériques - au sein de nos structures.
2. Mieux comprendre les menaces de surveillance pesant sur les échanges numériques.
3. Découvrir ou mieux comprendre des bonnes pratiques permettant d'améliorer la sécurité de nos activités informatiques.
4. Améliorer ses capacités à diffuser et faciliter l'adoption d'une évolution des pratiques de sécurisation dans ses organisations.

➔ Méthode mobilisée et méthode d'évaluation

La formation est animée de façon à permettre à chacun·e de partir de ses besoins en les partageant avec les autres participant·e·s afin de construire une analyse commune. Un éclairage méthodologique et technique adapté au niveau des participant·es est assuré par les formateur·ices.

Chaque temps est rythmé par des apports théoriques, de l'expérimentation collective et des travaux en petits ou grand groupe. Tous ces temps se déroulent de façon participative, de manière à s'appuyer sur l'expérience et les savoirs des

participant·es et d'être en mesure de répondre à leurs attentes, besoins et interrogations. Une évaluation des connaissances est réalisée en amont, puis à mi-parcours et à la clôture de l'action de formation.

➔ Déroulé

- Les enjeux de la surveillance, à l'échelle individuelle et collective : éléments de compréhension politiques, juridiques et techniques (éléments de compréhension sur le fonctionnement des réseaux, des ordinateurs/téléphones et des échanges d'informations en ligne).
- Un cadre à la sécurisation des pratiques, la réduction des risques : une approche collective et de soin.
- Modélisation de la menace et les processus de planification de sécurité opérationnelle.
- Pratiques courantes de sécurisation informatique / « gestes barrières numérique ». Mots de passe, sauvegarde, configuration, etc.
- Principes et logiques de sécurisation des pratiques et logiques de mise en place d'évolution des outils face aux contraintes.
- État des lieux de nos pratiques numériques, individuelles et collectives.
- Présentation et analyse autour d'outils numériques spécifiques utilisés ou non et analyse de leurs intérêts et leurs limites.
- Enjeux juridiques spécifiques sur la protection des données.
- Prise en main de certains outils de protection des informations (navigateur TOR, chiffrement de données, outils de protections des communication).
- Échanges et accompagnement éventuel sur des enjeux concrets liés aux problématiques des participant·es (outils, enjeux juridiques, diffusion au sein d'une organisation...).

➔ Pré-requis

Il est préférable (mais non obligatoire) de disposer d'un micro-ordinateur équipé d'un système d'exploitation à jour, et d'en avoir un usage courant pour pouvoir réaliser certaines des expérimentations et découvertes d'outils proposées.

La fiche « [FormationsNumeriques_PrerequisMateriel_ritimo_23.pdf](#) », détaille les équipements matériels et logiciels nécessaires pour suivre cette formation, et précise les points d'attention y afférents.

➔ Informations pratiques

▀ **Modalité de formation** : en présentiel

▀ **Lieu** : au CICP, 21ter rue Voltaire, 75011 PARIS

▀ **Horaires** : de 9h30 à 18h

▀ **Inscrit·es minimum** : 6 personnes

▀ **Inscrit·es maximum** : 18 personnes

▀ **Date limite d'inscription** : 7 mars 2023

▀ **Formateur·rices/intervenant·es** : Mélissa Richard, chargée d'animation numérique pour le réseau **ritimo**, et Sylvain Steer, militant engagé dans la défense des libertés en ligne et hors ligne, juriste bidouilleur, auteur du "Guide de Survie des Aventuriers du Net" (édité par l'association CECIL).

▀ **Accessibilité** :

Toutes les salles accueillant nos formations sont accessibles aux personnes à mobilité réduite.

Si vous avez d'autres besoins nécessitant que nous adaptions nos modalités pédagogiques, il suffit de nous écrire à l'adresse de contact mentionnée dans la fiche

de présentation ou en le précisant lors de remplir le formulaire de demande d'inscription.

➔ **Frais pédagogiques :**

- ▣ 30 € - Étudiant·es et chômeur·ses (sur justificatif) ;
- ▣ 60 € - Membres et relais du réseau **ritimo** ou de la Coredem ;
- ▣ 80 € - Bénévoles, volontaires du milieu associatif ;
- ▣ 600 € - Salarié·es bénéficiaires de la formation professionnelle.

➔ **Formulaire de demande d'inscription en ligne :**

Pour vous inscrire, merci de compléter le [formulaire d'inscription](#).

➔ **Contact :**

Mélissa Richard, chargée d'animation numérique pour le réseau ritimo,
par courriel (numerique (chez) ritimo.org) ou au téléphone (01.44.64.74.16)