DESPY - EDITION ENRICHIE 2026

LE GUIDE COMPLET

Ma protection numérique.

Reconnaître les arnaques. Sécuriser ses appareils.
Protéger sa famille en ligne. Sans jargon.

9	45	6	107
modules	quiz	fiches mémo	pages

✓ Garantie 30 jours satisfait ou remboursé

✓ Mises à jour gratuites 1 an

despy.fr

29,90 EUR

CE LIVRET APPARTIENT À

Mon parcours cybersécurité Despy

NOM ET PRÉNOM

_____

DATE DE REMISE

_____

INTERVENANT DESPY

_____

Ce livret accompagne votre formation Despy.
Conservez-le précieusement comme référence.

despy.fr · contact.despy@gmail.com · 06 89 14 83 95

SOMMAIRE

9 modules pour maîtriser votre protection numérique

6

Les achats en ligne en sécurité

L'e-commerce est entré dans nos vies. Mais entre les faux sites, les arnaques sur les mark...

7

Réseaux sociaux : ce qu'il ne faut jamais partager

Vos publications, vos photos, votre liste d'amis : tout ça est exploitable. Cybercriminels...

8

Que faire si je me fais pirater ?

Malgré toutes les précautions, ça peut arriver. L'important n'est pas d'éviter à 100% (imp...

9

Arnaques par Intelligence Artificielle

Les escrocs utilisent l'IA pour écrire des messages parfaits, cloner des voix et fabriquer de fausses vidéos...

INTRODUCTION

Qu'est-ce que la cybersécurité ?

La cybersécurité, c'est l'ensemble des bons réflexes et des outils qui protègent votre vie numérique : vos comptes, vos appareils, votre argent et vos données personnelles.

Aujourd'hui, votre téléphone contient autant d'informations que votre coffre-fort. Et chaque jour, des milliers de personnes essaient d'y entrer sans autorisation.

LES 3 PILIERS

1. **DÉTECTER**
   Reconnaître les arnaques avant qu'elles ne piègent (email qui presse, SMS d'inconnu, appel qui imite la banque).
2. **PRÉVENIR**
   Mettre en place les bons réflexes au quotidien (mots de passe solides, double authentification, mises à jour).
3. **RÉAGIR**
   Savoir quoi faire si l'incident arrive (couper l'accès, contacter la banque, changer ses mots de passe).

« La cybersécurité, ce n'est plus un sujet d'experts. C'est un réflexe de base. »

INTRODUCTION

Les chiffres qui doivent vous alerter

La cybercriminalité explose en France. Avant de commencer la formation, prenez 30 secondes pour mesurer l'ampleur du phénomène.

504 000

Français ont demandé de l'aide en 2024

Source : cybermalveillance.gouv.fr

1 sur 4

Français sera victime d'une cyberattaque cette année

Source : cybermalveillance.gouv.fr

+180 %

d'arnaques par SMS en un an

Source : Statistiques 2024

78 %

des cyberattaques particuliers commencent par un email

Source : ANSSI 2024

80 %

des piratages réussis sont liés à un mot de passe faible

Source : Verizon DBIR 2024

30 min

suffisent pour cracker un mot de passe à 8 caractères

Source : Hive Systems 2024

Ce livret est votre meilleure défense. Lisez-le, appliquez-le, partagez-le.

INTRODUCTION

Votre parcours en 4 étapes

Ce livret est conçu pour vous accompagner pas à pas. Suivez ces 4 étapes pour en tirer le maximum.

01

Faites les 9 modules dans l'ordre

Chaque module s'appuie sur le précédent. Comptez 15 à 20 minutes par module, soit environ 2 h 30 pour le livret complet.

02

Validez avec les quiz

À la fin de chaque module, un quiz de 5 questions ancre les bons réflexes. Les corrigés sont disponibles sur despy.fr, rubrique Formation.

03

Gardez les fiches mémo à portée

À la fin du livret, 6 fiches pratiques sont conçues pour être imprimées et gardées sous la main (frigo, bureau, portefeuille).

04

Restez équipé toute l'année

Les arnaques évoluent chaque semaine. Connectez-vous régulièrement à despy.fr pour des alertes en temps réel et l'aide de votre Conseiller.

Prêt ? Tournez la page et commencez par le Module 01.

Vous êtes à 2 h 30 d'une vie numérique mieux protégée.

01

MODULE 01 SUR 08

Reconnaître un email frauduleux

Les emails frauduleux (ou « phishing ») sont la première porte d'entrée des pirates. Apprenez à les détecter en 30 secondes, même quand ils imitent parfaitement votre banque, votre opérateur ou un service public.

À LA FIN DE CE MODULE, VOUS SAUREZ

- ✓ Identifier les 7 signes d'un email frauduleux
- ✓ Vérifier un expéditeur en 10 secondes
- ✓ Réagir correctement face à un email suspect
- ✓ Protéger votre boîte mail avec des règles simples

Pourquoi les emails frauduleux fonctionnent ?

En 2024, **78% des cyberattaques** contre les particuliers ont commencé par un email piégé. Les pirates jouent sur l'urgence, la peur ou la curiosité pour vous faire baisser votre garde.

3,4 Mds
d'emails frauduleux envoyés chaque jour

1 sur 4
est ouvert par le destinataire

12 sec
suffisent pour repérer une arnaque

Les 7 signes qui ne trompent jamais

1. L'adresse expéditeur ne correspond pas

C'est le premier réflexe. Avant de lire le contenu, regardez l'adresse complète de l'expéditeur (et pas seulement le nom affiché).

⚠ EXEMPLE D'ARNAQUE

Vous recevez un email de **"Banque Populaire"**.
Adresse réelle :

```
support@banquepopulaire-sec.com
```

Ce n'est pas le vrai domaine. Le vrai est **banquepopulaire.fr**.

2. Un sentiment d'urgence forcé

« Votre compte sera bloqué dans 24h », « Action immédiate requise »… L'urgence est créée pour vous empêcher de réfléchir.

⚡ PIÈGE CLASSIQUE

Aucun organisme sérieux ne menace par email. Si vraiment il y avait urgence, ils vous appelleraient.

3. Une demande d'informations sensibles

Votre banque, les impôts, la Sécu, ne vous demanderont **JAMAIS** par email :

- Votre mot de passe
- Votre code de carte bancaire
- Vos identifiants complets
- Une photo de votre carte d'identité

4. Des fautes d'orthographe ou de mise en page

Les grandes entreprises font relire leurs emails. Une faute, un logo flou, des espaces bizarres sont des signaux d'alarme.

5. Un lien qui ne mène pas où il prétend

Avant de cliquer, passez votre souris (sans cliquer !) sur le lien. L'adresse réelle apparaît en bas de votre écran.

VÉRIFICATION AVANT CLIC

Le texte affiche : **www.amazon.fr/commande**
Mais en survolant, on voit :

```
http://amaz0n-livraison.ru/login
```

6. Une pièce jointe que vous n'attendiez pas

Un email avec un **.zip**, **.exe** ou **.docm** non sollicité = danger immédiat. Ne l'ouvrez jamais.

7. Une formule d'appel impersonnelle

« Cher client », « Bonjour Monsieur/Madame » — votre banque connaît votre nom. Une formule générique est suspecte.

Les arnaques par email les plus courantes en 2025

📦 Faux colis

"Votre colis attend, payez 1,99€ pour la livraison"

🏦 Faux conseiller

"Activité suspecte sur votre compte, validez maintenant"

📺 Remboursement

"Impôts : remboursement de 437€ à valider"

🎁 Faux concours

"Vous avez gagné un iPhone 16 Pro !"

💼 Faux RH

"Bulletin de paie en pièce jointe, vérifiez vite"

⚠️ Faux antivirus

"Votre PC est infecté, téléchargez ce nettoyeur"

✓ MA ROUTINE ANTI-PHISHING

- [ ] Je vérifie toujours l'adresse complète de l'expéditeur
- [ ] Je ne clique jamais sur un lien sous le coup de l'urgence
- [ ] Je passe ma souris sur les liens avant de cliquer
- [ ] Je n'ouvre pas les pièces jointes inattendues
- [ ] En cas de doute, je contacte l'expéditeur par téléphone
- [ ] Je signale les emails frauduleux à signal-spam.fr

Que faire si j'ai cliqué par erreur ?

Pas de panique — voici les 4 étapes immédiates :

1. **Déconnectez-vous d'Internet** immédiatement (mode avion ou débrancher la box)
2. **Changez vos mots de passe** depuis un autre appareil sain
3. **Appelez votre banque** si vous avez communiqué des infos bancaires
4. **Faites un scan antivirus complet** avant de vous reconnecter

💡 **ASTUCE DESPY**

Vous avez un doute sur un email ? Transférez-le au Conseiller Despy depuis votre espace client. Réponse en quelques secondes, sans jugement.

POUR ALLER PLUS LOIN

L'arnaque "au Président"

Une variante sophistiquée vise les entrepreneurs : un faux email du patron demandant un virement urgent à un fournisseur. En 2023, 320 millions d'euros ont été détournés en France de cette manière. La règle d'or : tout virement urgent doit être confirmé par téléphone, jamais par email.

QUIZ DE VALIDATION

Testez vos acquis

1 Vous recevez un email de votre banque qui demande de cliquer sur un lien pour 'valider votre compte sous 24h'. Quelle est la bonne réaction ?

A Cliquer rapidement avant la fermeture du compte

B Ne pas cliquer et appeler votre banque directement

C Répondre à l'email en demandant confirmation

2 **Comment vérifier qu'un lien dans un email est sûr avant de cliquer ?**

A Cliquer et voir où il mène

B Passer la souris dessus sans cliquer pour voir l'URL réelle

C Le copier-coller dans une barre de recherche

3 **Un email impersonnel commençant par 'Cher client' est plus suspect qu'un email avec votre vrai nom.**

A Vrai — votre banque connaît votre nom

B Faux — c'est juste plus poli

C Cela dépend de l'expéditeur

4 **Vous recevez une pièce jointe inattendue d'un collègue. Que faire ?**

- **A** L'ouvrir, c'est un collègue de confiance
- **B** Vérifier avec lui par téléphone ou en vrai avant d'ouvrir
- **C** L'enregistrer puis l'ouvrir plus tard

5 **Quel organisme ne vous demandera JAMAIS votre mot de passe par email ?**

- **A** Votre banque uniquement
- **B** Les impôts uniquement
- **C** AUCUN organisme officiel ne le fait par email

i RÉPONSES

Retrouvez les corrigés et le quiz interactif sur votre espace client Despy : **despy.fr** → Formation → Module 01.

02

MODULE 02 SUR 08

Les arnaques par SMS

Le SMS frauduleux (smishing) a explosé en 2024 : +180% en un an. Plus court qu'un email, plus direct, il joue sur la confiance que nous accordons au mobile. Apprenez à détecter ces messages en 5 secondes.

À LA FIN DE CE MODULE, VOUS SAUREZ

- ✓ Reconnaître un SMS frauduleux au premier coup d'œil
- ✓ Identifier les 5 scénarios d'arnaques les plus répandus
- ✓ Réagir correctement sans paniquer
- ✓ Configurer votre téléphone pour bloquer ces SMS

Le SMS, l'arme préférée des arnaqueurs

Le SMS a un taux d'ouverture de **98%** contre 20% pour un email. C'est pourquoi les pirates l'adorent. Un SMS de votre "banque" à 22h, vous le lisez. Un SMS d'un "colis" qui attend, vous cliquez vite. C'est exactement ce qu'ils veulent.

+180%
d'arnaques par SMS entre 2023 et 2024

22h
l'heure préférée des arnaqueurs

3 sec
le temps moyen avant de cliquer

Les 5 SMS d'arnaque que vous allez recevoir

1. Le faux colis en attente

Le plus répandu. Vous attendez (peut-être) un colis, et hop : « Votre colis n'a pas pu être livré, payez les frais de port ici ».

⚠ **SMS FRAUDULEUX TYPE**

> "Votre colis Chronopost attend des frais de douane de 1,99€. Réglez ici sous 24h : chronopost-livraison.com/pay"

⚡ **RÉFLEXE VITAL**

Aucun transporteur ne demande de paiement par SMS. Les douanes encore moins. Si un colis est vraiment bloqué, vous recevez un avis de passage dans votre boîte.

2. La fausse banque

« Connexion suspecte détectée », « Validation de virement requise »… Le pirate veut que vous cliquiez pour saisir vos identifiants bancaires sur un faux site.

3. L'amende de stationnement

« Amende de 35€ à régler avant le… ». Faux. L'ANTAI n'envoie jamais d'amende par SMS. Vous recevez un avis papier ou via Mes Démarches.

4. Le "compte CPF" piraté

« Votre compte formation expire, activez-le ici ». Faux. Le CPF n'envoie pas ce genre de SMS.

5. Le service après-vente

« Cher client, votre abonnement expire, mettez à jour vos infos ». Souvent au nom de Netflix, Orange, Free… Le but est de récupérer votre carte bancaire.

Les 5 réflexes anti-SMS frauduleux

✓ **RÉFLEXES D'OR**

1. Ne JAMAIS cliquer sur un lien dans un SMS
2. Ne JAMAIS répondre, même pour dire "stop"
3. Vérifier le numéro émetteur (un vrai SMS officiel vient souvent d'un nom, pas d'un numéro)
4. Transférer au **33 700** (numéro gratuit anti-spam SMS)
5. Supprimer le SMS

Comment reconnaître un vrai SMS officiel ?

✓ EXEMPLE DE VRAI SMS DE BANQUE

"BANQUE_X : Code de validation : 458921. Ne le partagez avec personne. Valable 5 minutes."

Pas de lien. Pas de demande d'action. Juste un code qui répond à une action **que vous avez vous-même initiée**.

⚠ LE PIÈGE DU "CODE DE SÉCURITÉ"

Un arnaqueur peut vous appeler en disant qu'il est de votre banque et vous demander de lui lire un code reçu par SMS. NE LE FAITES JAMAIS. Ce code permet en réalité de valider sa propre connexion à votre compte.

Bloquer les SMS frauduleux sur votre téléphone

Sur iPhone

1. Réglages → Messages
2. Activer « Filtrer les expéditeurs inconnus »
3. Activer « Signaler les SMS indésirables »

Sur Android

1. Application Messages → Paramètres
2. Protection contre le spam → Activer
3. Bloquer les numéros inconnus

✓ MA CHECKLIST ANTI-SMS

- [ ] J'ai activé le filtre anti-spam SMS sur mon téléphone
- [ ] Je ne clique JAMAIS sur un lien dans un SMS
- [ ] Je ne donne JAMAIS un code reçu par SMS à quelqu'un au téléphone
- [ ] Je transfère les SMS suspects au 33 700
- [ ] Je vérifie l'expéditeur avant de réagir à un SMS

BON À SAVOIR

Le 33 700, votre allié gratuit

C'est le numéro officiel de signalement des SMS et appels indésirables, en partenariat avec les opérateurs et le gouvernement. Transférez-y tout SMS suspect : c'est gratuit, anonyme, et ça aide à faire fermer les réseaux frauduleux. En 2024, plus de 6 millions de SMS y ont été signalés.

QUIZ DE VALIDATION

Testez vos acquis

1 Vous recevez un SMS : 'Votre colis est en attente, payez 1,99€ ici'. Que faire ?

- A Cliquer pour payer rapidement
- B Ignorer et supprimer le SMS
- C Répondre 'STOP'

2 Votre banque vous appelle et demande de leur lire un code reçu par SMS. Que faire ?

- A Lui donner, c'est votre banque
- B Raccrocher et rappeler votre banque vous-même
- C Lui demander de prouver son identité

3 **À quel numéro signaler un SMS frauduleux ?**

- A Le 17 (police)
- B Le 33 700 (anti-spam SMS)
- C Le 3949 (renseignements)

4 **Un vrai SMS officiel contient généralement…**

- A Un lien vers un site et une demande d'action urgente
- B Juste un code de validation, sans lien
- C Une longue explication détaillée

5 **Pour bloquer les SMS frauduleux sur iPhone, on doit activer…**

A L'antivirus

B Le filtre des expéditeurs inconnus

C Le mode avion

i RÉPONSES

Retrouvez les corrigés et le quiz interactif sur votre espace client Despy : **despy.fr** → Formation → Module 02.

03

MODULE 03 SUR 08

Sécuriser ses mots de passe

Vos mots de passe sont les clés de votre vie numérique. En 2024, 80% des piratages réussis ont exploité un mot de passe trop faible ou réutilisé. Voici comment créer des mots de passe inviolables sans devenir fou.

À LA FIN DE CE MODULE, VOUS SAUREZ

- ✓ Comprendre ce qui rend un mot de passe vraiment fort
- ✓ Créer une méthode personnelle facile à retenir
- ✓ Utiliser un gestionnaire de mots de passe en 5 minutes
- ✓ Vérifier si vos mots de passe ont fuité sur Internet

Le mot de passe : le maillon le plus faible

Un mot de passe faible peut être cassé en quelques secondes. « 123456 » et « password » figurent encore en tête des mots de passe utilisés en France en 2024. Pendant ce temps, 4,7 milliards d'identifiants ont fuité sur le dark web.

2 sec
pour casser "password123"

5 ans
pour casser un bon mot de passe

75%
des Français réutilisent le même mot de passe

Ce qui fait un BON mot de passe

✓ LES 4 RÈGLES D'OR

1. **Long** : minimum 12 caractères (plus c'est long, plus c'est fort)
2. **Mélangé** : majuscules, minuscules, chiffres, symboles
3. **Unique** : un mot de passe différent par site
4. **Imprévisible** : pas votre date de naissance ni le nom de votre chien

La méthode de la "phrase de passe"

Au lieu d'un mot, prenez une phrase facile à retenir et transformez-la.

EXEMPLE CONCRET

Phrase : **"J'ai adopté Médor en 2018 à Strasbourg !"**

Mot de passe :

`JaiAdopteMedor#2018Strasbourg!`

Résultat : **30 caractères**, mémorisable, ultra-fort.

Les pires erreurs à éviter

❌ **"azerty", "123456"**

Cassés en moins d'une seconde

❌ **Votre prénom + année**

"Marie1985" se trouve sur Facebook

❌ **Nom du chien, conjoint**

Visible sur vos réseaux sociaux

❌ **Un seul mot de passe**

Tout tombe en cascade

❌ **Noté sur un post-it**

Visible par tout visiteur

❌ **Envoyé par email**

Reste dans la boîte à jamais

Le gestionnaire de mots de passe : votre meilleur ami

Un gestionnaire est un coffre-fort numérique. Vous retenez UN seul mot de passe maître, il gère tout le reste pour vous.

💡 **NOS GESTIONNAIRES RECOMMANDÉS**

Gratuit : Bitwarden (open source, en français)
Premium : 1Password ou Dashlane (interface très simple)
Intégré : iCloud Keychain (iPhone) ou Google Password Manager (Android)

Vérifier si vos mots de passe ont fuité

Le site **haveibeenpwned.com** permet de vérifier en quelques secondes si votre email apparaît dans une fuite de données connue.

SERVICE INCLUS AVEC DESPY

Surveillance dark web automatique

Despy vérifie chaque mois si votre email a fuité et vous alerte immédiatement. Tableau de bord dans votre espace client.

Combien de mots de passe différents avoir ?

Au minimum, séparez vos comptes en 3 catégories :

- **Critiques** (banque, impôts, email principal) : 1 mot de passe unique par compte
- **Importants** (réseaux sociaux, Amazon, Netflix) : 1 mot de passe unique par compte
- **Secondaires** (forums, sites occasionnels) : peuvent partager le même, mais différent des autres catégories

✓ MA CHECKLIST MOTS DE PASSE

- [ ] Mon mot de passe email principal fait plus de 12 caractères
- [ ] Mon mot de passe banque est unique (utilisé nulle part ailleurs)
- [ ] J'ai installé un gestionnaire de mots de passe
- [ ] J'ai vérifié mes emails sur haveibeenpwned.com
- [ ] Je n'ai aucun mot de passe sur un post-it ou dans un fichier "passwords.txt"

MYTHE CONTRE RÉALITÉ

"Je change mon mot de passe tous les 3 mois"

Cette recommandation est dépassée depuis 2017. Forcer des changements fréquents pousse les utilisateurs à utiliser des variations faibles (motdepasse1, motdepasse2…). Mieux vaut UN mot de passe fort, gardé longtemps, et changé UNIQUEMENT s'il y a suspicion de compromission.

QUIZ DE VALIDATION

Testez vos acquis

1 **Quel mot de passe est le plus sûr ?**

A Marie1985!

B VinIv@VendrediSoir2024

C MotDePasse#

2 **Combien de mots de passe différents devriez-vous avoir au minimum ?**

A Un seul, bien retenu

B Trois par catégorie de sites

C Un unique par compte sensible

3 **Qu'est-ce qu'un gestionnaire de mots de passe ?**

- **A** Un coffre-fort numérique pour stocker vos mots de passe
- **B** Un logiciel qui génère des mots de passe au hasard
- **C** Un site qui vérifie vos mots de passe

4 **Sur quel site vérifier si votre email a fuité ?**

- **A** mots-de-passe.fr
- **B** haveibeenpwned.com
- **C** google.com/passwords

5 **Faut-il changer son mot de passe tous les 3 mois ?**

- **A** Oui, c'est la règle officielle
- **B** Non, mieux vaut un bon mot de passe gardé longtemps
- **C** Tous les ans suffit

i RÉPONSES

Retrouvez les corrigés et le quiz interactif sur votre espace client Despy : **despy.fr** → Formation → Module 03.

04

MODULE 04 SUR 08

La double authentification

Même avec un mot de passe parfait, il peut être volé. La double authentification (2FA) ajoute une seconde clé : un code unique que seul vous pouvez recevoir. C'est la protection la plus efficace qui existe — et elle est gratuite.

À LA FIN DE CE MODULE, VOUS SAUREZ

- ✓ Comprendre comment fonctionne la 2FA
- ✓ Activer la 2FA sur vos comptes critiques en 5 minutes
- ✓ Choisir la meilleure méthode (SMS, app, clé physique)
- ✓ Que faire si vous perdez votre téléphone

Pourquoi un mot de passe ne suffit plus

Imaginez votre maison avec une serrure ultra-sécurisée. Si quelqu'un vole votre clé, il entre. La double authentification, c'est ajouter un digicode après la serrure : sans le code, même avec la clé, impossible d'entrer.

> **i LE CHIFFRE QUI CHANGE TOUT**
>
> Selon Google, activer la double authentification bloque **99,9%** des piratages de compte automatisés. C'est la protection la plus efficace, et elle est gratuite.

Comment ça marche concrètement ?

Quand vous vous connectez à un compte protégé par 2FA :

1. Vous entrez votre identifiant + mot de passe (comme d'habitude)
2. Le site vous demande un code à 6 chiffres
3. Ce code arrive sur votre téléphone (par SMS, app ou clé physique)
4. Vous le saisissez, et vous êtes connecté

Sans votre téléphone, un voleur de mot de passe ne peut rien faire. Même si votre mot de passe est sur le dark web, votre compte reste protégé.

Les 3 méthodes de double authentification

1. Par SMS (la plus simple)

Vous recevez le code par SMS. Pratique, mais le moins sûr : un pirate peut détourner votre numéro (rare mais possible).

> ⚠ **QUAND L'UTILISER ?**
>
> Pour les comptes secondaires (réseaux sociaux, sites de e-commerce). Évitez-la pour votre banque et email principal.

2. Par application (recommandé)

Une application sur votre téléphone génère le code toutes les 30 secondes, même sans Internet ni réseau. C'est ce qu'on appelle un code TOTP.

> 💡 **APPLICATIONS RECOMMANDÉES (GRATUITES)**
>
> **Google Authenticator** — Très simple
> **Microsoft Authenticator** — Avec sauvegarde cloud
> **Authy** — Synchronisation multi-appareils
> **2FAS** — Open source, en français

3. Par clé physique (le plus sûr)

Une petite clé USB ou NFC (YubiKey, Titan…) qui sert de "preuve physique". Impossible à pirater à distance.

Coût : environ 50€. Recommandé pour les comptes vraiment critiques (crypto, comptes pros).

Sur quels comptes activer la 2FA en priorité ?

✓ MES COMPTES À PROTÉGER D'URGENCE

- [ ] Email principal (Gmail, Outlook, Yahoo…)
- [ ] Banques et comptes bancaires en ligne
- [ ] Impôts (impots.gouv.fr)
- [ ] France Connect / Ameli / Compte CPF
- [ ] Réseaux sociaux (Facebook, Instagram, LinkedIn)
- [ ] Amazon et autres sites avec votre carte bancaire enregistrée
- [ ] Apple ID / Google Account / Microsoft

Comment activer la 2FA en 5 minutes ?

Exemple sur Gmail :

1. Allez sur **myaccount.google.com**
2. Cliquez sur **Sécurité** dans le menu de gauche
3. Trouvez **"Validation en 2 étapes"**
4. Cliquez sur **"Activer"** et suivez les instructions

> ✓ **LE GESTE QUI SAUVE**
>
> Lors de l'activation, le service vous donne des **codes de récupération**. NOTEZ-LES sur papier et rangez-les dans un endroit sûr. Ils vous sauveront si vous perdez votre téléphone.

Que faire si je perds mon téléphone ?

C'est la peur de tout le monde, et c'est légitime. Voici les 3 solutions :

1. **Utiliser vos codes de récupération** (notés à l'activation)
2. **Avoir une méthode de secours** : un email secondaire ou un numéro de téléphone alternatif
3. **Utiliser une app avec sauvegarde cloud** (Authy, Microsoft Authenticator) qui retrouve vos codes sur un nouveau téléphone

Les pièges autour de la 2FA

⚡ **ARNAQUE CLASSIQUE : LE FAUX SUPPORT**

Quelqu'un appelle en se faisant passer pour votre banque, vous explique qu'il y a un problème et demande que vous lui lisiez le code de validation reçu par SMS. **NE DONNEZ JAMAIS CE CODE**. Aucun vrai support ne vous demandera jamais ça.

POUR ALLER PLUS LOIN

Le "SIM swap" : la nouvelle menace

Des pirates parviennent parfois à transférer votre numéro de téléphone sur leur propre SIM, en se faisant passer pour vous chez votre opérateur. C'est pourquoi la 2FA par SMS reste vulnérable. Si possible, privilégiez les apps comme Google Authenticator. Chez votre opérateur, demandez la mise en place d'un mot de passe pour toute modification de votre ligne.

QUIZ DE VALIDATION

Testez vos acquis

1 **Que signifie 'double authentification' ?**

- A Avoir deux mots de passe différents
- B Confirmer son identité avec un second élément (code, appli, clé)
- C Se connecter sur deux appareils en même temps

2 **Quelle méthode 2FA est la plus sûre ?**

- A SMS
- B Application authentificatrice
- C Clé physique de sécurité

3 **Que faire des codes de récupération donnés à l'activation ?**

A Les supprimer après lecture

B Les noter sur papier et les ranger en sécurité

C Les sauvegarder dans un email

4 **Un support technique vous appelle et demande votre code reçu par SMS. Que faire ?**

A Lui donner pour être aidé rapidement

B Raccrocher et rappeler le numéro officiel

C Lui demander de prouver son identité

5 **Activer la 2FA bloque combien de piratages selon Google ?**

A 50%

B 75%

C 99,9%

i RÉPONSES

Retrouvez les corrigés et le quiz interactif sur votre espace client Despy : **despy.fr** → Formation → Module 04.

05

MODULE 05 SUR 08

Protéger ses appareils

Votre téléphone, votre ordinateur, votre tablette contiennent toute votre vie : photos, contacts, banque, mots de passe. Voici comment les transformer en forteresses, sans devenir expert.

À LA FIN DE CE MODULE, VOUS SAUREZ

- ✓ Sécuriser son téléphone en 10 minutes
- ✓ Détecter un programme indésirable sur son appareil
- ✓ Faire les bonnes sauvegardes
- ✓ Choisir un bon antivirus (et savoir quand il est inutile)

Votre appareil, c'est votre vie numérique

Si quelqu'un avait accès à votre téléphone pendant 5 minutes, que pourrait-il faire ? Lire vos messages, accéder à vos comptes, récupérer vos photos, voler votre identité. La protection physique et logicielle de vos appareils est aussi importante que celle de votre logement.

Téléphone : les 7 réflexes essentiels

1. Verrouillez votre écran (vraiment)

Code à 6 chiffres minimum, ou empreinte digitale / reconnaissance faciale. Pas de "1234", pas de "0000", pas de schéma en L.

2. Activez le verrouillage automatique en 30 secondes

Réglages → Affichage → Verrouillage auto → 30 secondes. Plus le délai est court, mieux c'est.

3. Mettez à jour votre système

Chaque mise à jour corrige des failles de sécurité. Activer les mises à jour automatiques.

> ⚠ **TÉLÉPHONE TROP VIEUX ?**
>
> Si votre téléphone ne reçoit plus de mises à jour de sécurité (généralement 5-6 ans après sa sortie), il devient vulnérable. À terme, prévoyez de le remplacer.

4. N'installez que des applications officielles

Uniquement depuis l'App Store (iPhone) ou le Play Store (Android). Pas de fichiers APK trouvés en ligne, jamais.

5. Vérifiez les permissions des applications

Une lampe torche n'a pas besoin de votre localisation. Une calculatrice n'a pas besoin de vos contacts. Vérifiez régulièrement.

6. Activez la localisation à distance

Pour pouvoir retrouver, sonner ou effacer votre téléphone à distance s'il est perdu ou volé.

- **iPhone** : « Localiser » dans les réglages iCloud
- **Android** : « Localiser mon appareil » dans les réglages Google

7. Soyez attentif aux signes anormaux

⚡ SIGNES D'UN PROGRAMME INDÉSIRABLE

- **Batterie qui se vide vite**, même sans utilisation
- **Téléphone qui chauffe** sans raison
- **Forfait data qui explose**
- **Publicités qui apparaissent** hors des applications
- **Applications inconnues** que vous n'avez pas installées
- **Bruit étrange** pendant les appels

Ordinateur : sécuriser sans complications

Les 5 protections de base

1. **Compte avec mot de passe** (jamais de session ouverte sans protection)
2. **Système à jour** (Windows Update activé, macOS Software Update activé)
3. **Pare-feu activé** (par défaut sur Windows et Mac, vérifiez-le)
4. **Antivirus** (Windows Defender suffit pour 95% des particuliers)
5. **Sauvegardes régulières** (voir plus bas)

💡 **ANTIVIRUS : PAYANT OU GRATUIT ?**

Sur Windows 10/11 : Windows Defender (intégré, gratuit) est largement suffisant pour un usage personnel.
Sur Mac : la protection intégrée (XProtect) suffit aussi.
Vous n'avez besoin d'un antivirus payant que pour des usages très exposés (téléchargements fréquents, navigation à risque).

La sauvegarde : votre filet de sécurité

Si vous perdez votre téléphone, il est volé ou cassé, ou si vous attrapez un virus qui chiffre vos fichiers (ransomware), seule une sauvegarde récente vous sauvera.

La règle du 3-2-1

✓ **LA RÈGLE D'OR DES SAUVEGARDES**

3 copies de vos données importantes
2 supports différents (ex: PC + disque externe)
1 copie hors site (cloud ou chez un proche)

Solutions simples

- **iCloud** (iPhone) : 50 Go pour 0,99€/mois — automatique
- **Google One** (Android) : 100 Go pour 1,99€/mois
- **OneDrive** (Windows) : inclus avec Microsoft 365

- **Disque dur externe** : 1 To pour ~50€, à brancher chaque semaine

Tablette : les bonnes pratiques

Mêmes règles que pour le téléphone. Attention particulière si vous la prêtez aux enfants : créez un compte enfant avec restrictions.

✓ MA CHECKLIST APPAREILS

- [ ] Téléphone verrouillé avec code à 6 chiffres ou biométrie
- [ ] Verrouillage automatique en moins de 1 minute
- [ ] Mises à jour système activées en automatique
- [ ] Localisation à distance activée
- [ ] Sauvegarde cloud activée
- [ ] Ordinateur protégé par mot de passe à l'ouverture
- [ ] Antivirus actif (Defender ou autre)
- [ ] Sauvegarde mensuelle sur disque externe ou cloud

BON À SAVOIR

Wifi public : tous les pièges

Le Wifi gratuit du café ou de l'hôtel peut être piégé. Évitez d'y faire vos opérations bancaires ou d'y entrer des mots de passe. Si vraiment vous devez, activez votre 4G/5G à la place, ou utilisez un VPN (Mullvad, ProtonVPN sont reconnus). Pour 5€/mois, vous chiffrez toute votre connexion.

QUIZ DE VALIDATION

Testez vos acquis

1 Quel code de verrouillage est acceptable pour un téléphone ?

A 1234 (facile à retenir)

B Code à 6 chiffres + biométrie

C Schéma en L

2 **Que faire si votre téléphone chauffe et que la batterie se vide vite ?**

- **A** C'est normal, ne rien faire
- **B** Vérifier les applications récemment installées, possible programme indésirable
- **C** Acheter un nouveau téléphone

3 **Sur Windows 10/11, l'antivirus Windows Defender est…**

- **A** Insuffisant, il faut un antivirus payant
- **B** Largement suffisant pour un usage personnel
- **C** À désactiver pour éviter les conflits

4 **Quelle est la règle d'or des sauvegardes ?**

A Une copie sur clé USB suffit

B La règle 3-2-1 : 3 copies, 2 supports, 1 hors site

C Sauvegarder chaque semaine sur le cloud

5 **Faut-il faire ses opérations bancaires sur un Wifi public ?**

A Oui, c'est plus rapide

B Non, jamais — privilégier 4G/5G ou VPN

C Seulement sur des Wifi d'hôtels

i RÉPONSES

Retrouvez les corrigés et le quiz interactif sur votre espace client Despy : **despy.fr** → Formation → Module 05.

06

MODULE 06 SUR 08

Les achats en ligne en sécurité

L'e-commerce est entré dans nos vies. Mais entre les faux sites, les arnaques sur les marketplaces et les vols de carte bancaire, c'est un terrain miné. Apprenez à acheter sereinement.

À LA FIN DE CE MODULE, VOUS SAUREZ

- ✓ Reconnaître un site marchand fiable
- ✓ Identifier les arnaques de marketplaces (Vinted, Leboncoin…)
- ✓ Utiliser les bons moyens de paiement
- ✓ Faire valoir vos droits en cas de problème

Le piège des prix trop beaux pour être vrais

Un iPhone à 199€, des Nike à 39€, une PlayStation à 250€… Si le prix est anormalement bas, c'est une arnaque. Les pirates créent de faux sites copiant les vraies marques pour récupérer votre carte bancaire ou vous envoyer des contrefaçons (au mieux) ou rien du tout (au pire).

42%
des Français ont déjà été arnaqués en ligne

315€
le préjudice moyen par victime

+220%
de faux sites créés en 2024

Reconnaître un site marchand fiable

Les 5 signes d'un VRAI site

✓ À VÉRIFIER AVANT D'ACHETER

1. URL en **https://** (avec le cadenas)
2. Mentions légales complètes (SIRET, adresse, contact)
3. Conditions générales de vente accessibles
4. Avis clients sur des sites tiers (Trustpilot, Avis Vérifiés)
5. Plusieurs moyens de paiement proposés

Les 5 signes qui doivent vous alarmer

⚡ ALERTES ROUGES

1. Prix anormalement bas (-50% sur du neuf)
2. Site récent (date de création visible sur whois.com)
3. Fautes d'orthographe sur le site
4. Adresse de contact uniquement gmail.com ou yahoo.com
5. Pression à l'achat ("Plus que 1 exemplaire !", "Offre fin dans 10:00")

Vérifier un site en 30 secondes

Avant tout achat sur un site inconnu :

1. Allez sur **scamadviser.com** et tapez l'adresse du site
2. Consultez les avis sur **trustpilot.com**
3. Tapez "nom du site + arnaque" sur Google
4. Vérifiez la date de création du domaine sur **whois.com**

Les arnaques des marketplaces

Sur Leboncoin, Vinted, Marketplace…

Les vendeurs malhonnêtes utilisent des techniques bien rodées :

💳 Faux paiement

"Je vous envoie un lien sécurisé pour le paiement"

📦 Faux transporteur

Email type "Chronopost" pour confirmer une livraison fictive

💰 Trop-perçu

"Je vous ai envoyé 200€ de trop, remboursez-moi"

🌐 Hors plateforme

"On finalise par WhatsApp pour éviter les frais"

⚠ **RÈGLE D'OR DES MARKETPLACES**

Restez TOUJOURS sur la plateforme officielle. Ne payez jamais en dehors. Méfiez-vous des liens envoyés en message privé. Si on vous propose un paiement par PayPal "ami et famille", refusez : pas de protection acheteur.

Les moyens de paiement par ordre de sécurité

🥇 Le top : carte virtuelle (e-Carte Bleue)

Votre banque vous génère un numéro de carte unique pour chaque achat. Si volé, il est inutilisable ailleurs. Disponible chez la plupart des banques (souvent gratuit).

🥈 PayPal

Vos infos bancaires ne sont jamais transmises au vendeur. Très bonne protection acheteur en cas de litige.

🥉 Carte bancaire classique

Bien protégée par la double validation (3D Secure). En cas de fraude, votre banque vous rembourse (loi Hamon).

⚠️ À éviter

- **Virement bancaire** : aucune protection, aucun retour possible
- **Western Union, MoneyGram** : 99% des demandes en marketplace sont des arnaques
- **Cryptomonnaies** : transactions irréversibles, idéales pour les arnaqueurs
- **PayPal "Amis et famille"** : pas de protection acheteur

Vos droits en cas de problème

> **ℹ LE DROIT DE RÉTRACTATION**
>
> Pour tout achat en ligne en France, vous disposez de **14 jours** pour changer d'avis et être remboursé intégralement (sauf cas particuliers : périssables, sur-mesure…). C'est la loi.

En cas de fraude carte bancaire :

1. Faire opposition immédiatement auprès de votre banque
2. Déposer plainte (en ligne sur masecurite.interieur.gouv.fr)
3. Demander remboursement à votre banque (vous êtes remboursé sous 30 jours selon la loi)

✓ MA CHECKLIST ACHATS EN LIGNE

- [ ] J'ai vérifié le site sur Trustpilot avant d'acheter
- [ ] L'URL commence bien par https:// avec le cadenas
- [ ] J'utilise une e-Carte Bleue ou PayPal en priorité
- [ ] Sur marketplace, je reste sur la plateforme officielle
- [ ] Je connais mon droit de rétractation de 14 jours
- [ ] J'ai activé les alertes SMS sur ma carte bancaire

LE SAVIEZ-VOUS ?

3D Secure : votre filet de sécurité

Depuis 2021, tout paiement en ligne de plus de 30€ doit obligatoirement déclencher une vérification supplémentaire (code SMS, validation dans l'app bancaire). Si un site ne demande JAMAIS cette validation pour un montant supérieur à 30€, c'est suspect. C'est l'une des protections les plus efficaces contre la fraude.

QUIZ DE VALIDATION

Testez vos acquis

1 Un site propose un iPhone neuf à 199€. Que faire ?

A Acheter vite avant que ça remonte

B Vérifier l'authenticité du site, c'est probablement une arnaque

C Comparer avec d'autres sites

2 Sur Leboncoin, un acheteur vous propose de finaliser sur WhatsApp pour 'éviter les frais'. Que faire ?

A Accepter pour économiser

B Refuser et rester sur la plateforme officielle

C Demander une réduction

3 **Quel moyen de paiement offre la meilleure protection ?**

- A Le virement bancaire
- B L'e-Carte Bleue (numéro unique par achat)
- C Le mandat cash

4 **Combien de jours avez-vous pour vous rétracter d'un achat en ligne ?**

- A 7 jours
- B 14 jours
- C 30 jours

5 **Que faire en cas de fraude sur votre carte bancaire ?**

A Attendre que ça se règle

B Faire opposition immédiatement et déposer plainte

C Changer de banque

i RÉPONSES

Retrouvez les corrigés et le quiz interactif sur votre espace client Despy : **despy.fr** → Formation → Module 06.

07

MODULE 07 SUR 08

Réseaux sociaux : ce qu'il ne faut jamais partager

Vos publications, vos photos, votre liste d'amis : tout ça est exploitable. Cybercriminels, recruteurs, voisins curieux ou pire — les ennuis commencent souvent par une simple photo de vacances mal partagée.

À LA FIN DE CE MODULE, VOUS SAUREZ

- ✓ Régler la confidentialité de vos comptes en 5 minutes
- ✓ Identifier ce qu'il ne faut jamais publier
- ✓ Repérer les faux comptes et profils piégés
- ✓ Protéger vos enfants sur les réseaux sociaux

Ce que vos publications disent vraiment de vous

Une photo de vacances = vous êtes absent de chez vous (cambriolages organisés via Instagram). Une photo de votre voiture = numéro de plaque exploitable. Le nom de votre chien = potentiel mot de passe. Les réseaux sociaux sont une mine d'or pour les escrocs.

> ⚡ **LE CAS RÉEL**
>
> En 2024, 31% des cambriolages ont été précédés d'une surveillance des réseaux sociaux de la victime. "Je suis à Bali jusqu'au 28 août" : une bénédiction pour les cambrioleurs.

Les 10 choses à ne JAMAIS publier

1. **Vos vacances en temps réel** — publiez après votre retour
2. **Votre adresse précise** ni votre numéro de plaque
3. **Vos billets de spectacle ou cartes d'embarquement** (codes-barres exploitables)
4. **Votre nouveau permis ou carte bancaire**, même floutée

5. **Le nom de jeune fille de votre mère** (souvent une question de récupération de compte)
6. **Votre date et lieu de naissance complets**
7. **Les noms de vos enfants et leur école**
8. **Le nom de votre animal** (souvent utilisé en mot de passe)
9. **Vos horaires habituels** ("Toujours au resto le vendredi soir !")
10. **Vos plaintes contre votre employeur** ou autres infos pro sensibles

Régler la confidentialité : 5 minutes par réseau

Facebook

1. Paramètres → Confidentialité → Vérification de confidentialité
2. Limiter "Qui peut voir vos publications" à "Amis uniquement"
3. Désactiver "Le moteur de recherche peut me trouver"
4. Désactiver la reconnaissance faciale

Instagram

1. Paramètres → Confidentialité → Compte privé (activer)
2. Désactiver "Affichage de l'activité"
3. Désactiver "Partage de localisation dans Stories"

LinkedIn

1. Paramètres → Confidentialité → Visibilité du profil
2. Désactiver "Notifier mon réseau lors des changements de profil"
3. Limiter qui peut voir votre adresse email

TikTok

1. Paramètres → Confidentialité → Compte privé
2. Désactiver le téléchargement de vos vidéos
3. Limiter les commentaires aux abonnés

Reconnaître un faux profil

⚠ SIGNES D'UN FAUX PROFIL

- **Très peu de photos** ou seulement des photos professionnelles
- **Compte créé récemment** (date de création visible)
- **Peu d'amis ou des amis "exotiques"** sans cohérence
- **Demande d'ami sans raison** apparente
- **Compliments excessifs** dès les premiers messages
- **Évite les appels vidéo** ou les rencontres

L'arnaque sentimentale (Brouteur)

Quelqu'un de "très bien" vous contacte sur Facebook ou un site de rencontre. Il devient rapidement très proche, vous parle d'amour, puis a "un problème" qui nécessite votre aide financière. Vous envoyez de l'argent. Vous ne reverrez jamais cette personne.

⚡ **LES RÈGLES D'OR**

1. Une rencontre en ligne qui demande de l'argent = arnaque, dans 100% des cas
2. Refus d'appel vidéo = arnaque
3. Histoire impliquant l'armée, des médecins, des héritages = arnaque

Protéger ses enfants sur les réseaux sociaux

Les règles à instaurer

- **Âge minimum 13 ans** pour la plupart des réseaux (parfois 15 en Europe)
- **Comptes privés** obligatoires
- **Localisation désactivée** partout
- **Discussion ouverte** sur les risques (cyberharcèlement, sextorsion)

- **Le téléphone hors de la chambre** la nuit

ℹ CONTRÔLE PARENTAL

Apple (Temps d'écran) et Google (Family Link) proposent des outils gratuits pour limiter le temps d'écran, contrôler les applications installées et voir l'activité. Indispensables pour les moins de 16 ans.

Photo de famille publiée : les dangers

Publier des photos d'enfants pose plusieurs risques :

- Récupération des images à des fins illégales
- Géolocalisation possible via les métadonnées de la photo
- Identification facile (visages, école visible en arrière-plan…)
- L'enfant n'a pas donné son consentement

💡 ALTERNATIVE

Pour partager des photos avec votre famille, créez un album partagé privé sur iCloud, Google Photos ou Famicity. Personne d'autre ne peut y accéder.

✓ MA CHECKLIST RÉSEAUX SOCIAUX

- [ ] Tous mes comptes sont en mode "privé"
- [ ] Je n'affiche jamais ma position en temps réel
- [ ] Je ne publie aucune photo de carte d'identité, billet, etc.
- [ ] Je ne mets pas le nom complet de mes enfants en ligne
- [ ] Je vérifie chaque demande d'ami (pas d'inconnus)
- [ ] Je ne réponds jamais à des messages d'inconnus charmants
- [ ] Le contrôle parental est activé sur les téléphones des enfants

BON À SAVOIR

Le "droit à l'oubli"

Vous pouvez demander à Google et autres moteurs de recherche de supprimer un résultat vous concernant. Allez sur **support.google.com/legal** et faites votre demande. C'est gratuit, et la loi vous donne raison dans la plupart des cas. Vous pouvez aussi demander la suppression de vos données à n'importe quel site français (RGPD, article 17).

QUIZ DE VALIDATION

Testez vos acquis

1 Publier ses photos de vacances en temps réel sur Instagram, c'est…

A Sans risque

B Dangereux : ça signale votre absence aux cambrioleurs

C Recommandé pour faire plaisir aux amis

2 Quelle info est PARTICULIÈREMENT à éviter sur les réseaux sociaux ?

A Le nom de votre animal (souvent un mot de passe)

B Votre plat préféré

C Votre film préféré

3 **Quelqu'un rencontré en ligne vous demande de l'argent. C'est…**

- A Une marque de confiance
- B Une arnaque, dans 100% des cas
- C À évaluer au cas par cas

4 **Quel mode activer sur tous les comptes sociaux ?**

- A Mode public
- B Mode privé
- C Mode invité

5 **Pour partager des photos d'enfants en sécurité, mieux vaut…**

A Les publier sur Facebook avec un public restreint

B Utiliser un album partagé privé (iCloud, Google Photos)

C Les envoyer par email

i RÉPONSES

Retrouvez les corrigés et le quiz interactif sur votre espace client Despy : **despy.fr** → Formation → Module 07.

08

MODULE 08 SUR 08

Que faire si je me fais pirater ?

Malgré toutes les précautions, ça peut arriver. L'important n'est pas d'éviter à 100% (impossible) mais de réagir vite et bien. Voici votre plan d'action complet — gardez ce chapitre sous la main.

À LA FIN DE CE MODULE, VOUS SAUREZ

- ✓ Reconnaître les signes d'un piratage
- ✓ Réagir en moins de 30 minutes pour limiter les dégâts
- ✓ Récupérer un compte piraté
- ✓ Faire valoir vos droits et obtenir réparation

Comment savoir que je suis piraté ?

Le piratage n'est pas toujours évident. Parfois, des semaines passent avant qu'on s'en rende compte. Voici les signes qui doivent vous alerter immédiatement.

Signes sur vos comptes en ligne

- Connexions depuis des lieux ou appareils inconnus
- Messages envoyés en votre nom que vous n'avez pas écrits
- Mot de passe qui ne fonctionne plus
- Email de "confirmation de changement" que vous n'avez pas demandé
- Amis qui vous signalent un comportement étrange de votre compte
- Achats ou virements que vous n'avez pas effectués

Signes sur votre appareil

- Ralentissement soudain et important
- Applications inconnues installées
- Batterie qui se vide anormalement vite
- Données mobiles consommées massivement
- Pop-ups et publicités hors navigateur
- Webcam qui s'allume seule

PLAN D'URGENCE en 30 minutes

⚡ ACTION IMMÉDIATE (5 PREMIÈRES MINUTES)

1. Déconnectez l'appareil concerné d'Internet (mode avion, débrancher la box)
2. Depuis un AUTRE appareil sûr, changez le mot de passe du compte concerné
3. Activez la double authentification si pas déjà fait
4. Déconnectez toutes les sessions actives sur ce compte

⚠ ÉTAPE 2 (15 MINUTES SUIVANTES)

5. Si compte email : changez les mots de passe de TOUS les comptes liés
6. Si compte bancaire : appelez votre banque, faites opposition
7. Si réseaux sociaux : prévenez vos contacts du piratage
8. Vérifiez les paramètres : adresse email de récupération, numéro de téléphone associés

✓ ÉTAPE 3 (DANS LA JOURNÉE)

9. Lancez un scan antivirus complet sur tous vos appareils
10. Déposez plainte (en ligne sur masecurite.interieur.gouv.fr)
11. Signalez sur cybermalveillance.gouv.fr
12. Si paiement frauduleux : déclarez à votre banque sous 13 mois maximum

Récupérer un compte piraté

Gmail / Compte Google

1. Allez sur **accounts.google.com/signin/recovery**
2. Saisissez votre email
3. Suivez les étapes (questions de sécurité, email de récupération, téléphone…)
4. Une fois récupéré : changez le mot de passe, activez la 2FA, vérifiez les filtres de messagerie

Facebook / Instagram

1. Allez sur **facebook.com/hacked**
2. "Mon compte a été piraté" → suivez les étapes
3. Pour Instagram : tapez sur "Mot de passe oublié" puis "Besoin d'aide"

Compte bancaire

1. Appelez immédiatement le service "opposition" de votre banque (24h/24)
2. Faites bloquer toutes les cartes et l'accès internet
3. Demandez la régénération de tous les codes
4. Déposez plainte AVANT de demander remboursement

Le ransomware : la crise majeure

Si vos fichiers sont chiffrés et qu'on vous demande une rançon pour les récupérer :

⚡ **RÈGLES D'OR FACE À UN RANSOMWARE**

1. NE PAYEZ JAMAIS la rançon — vous financez le crime et n'avez aucune garantie de récupérer vos fichiers
2. Déconnectez immédiatement l'ordinateur du réseau
3. Allez sur **nomoreransom.org** — des outils de déchiffrement gratuits existent pour de nombreux ransomwares
4. Sinon, la seule solution est de tout effacer et restaurer depuis une sauvegarde

Les organismes qui peuvent vous aider

ℹ **VOS CONTACTS D'URGENCE**

17 — Police, en cas d'urgence
3018 — Aide aux victimes de violences numériques (gratuit, anonyme)
0 805 805 817 — Info Escroqueries (gratuit, lun-ven 9h-18h30)
cybermalveillance.gouv.fr — Plateforme officielle d'assistance
signal-spam.fr — Pour signaler emails et SMS frauduleux
33700 — Anti-spam SMS (gratuit)

Vos droits en cas de fraude bancaire

La loi est de votre côté :

- **Article L133-18 du Code monétaire** : la banque doit vous rembourser les opérations non autorisées
- **Délai** : sous 30 jours, sauf en cas de négligence grave de votre part
- **Charge de la preuve** : c'est à la banque de prouver votre négligence, pas l'inverse
- **Médiation** : si désaccord, saisissez le médiateur bancaire (gratuit)

Et après ? Les bonnes pratiques

✓ REPRENDRE SA SÉCURITÉ EN MAIN

- [ ] Tous mes mots de passe ont été changés
- [ ] La 2FA est activée sur tous mes comptes critiques
- [ ] J'ai vérifié toutes mes sessions actives
- [ ] J'ai un gestionnaire de mots de passe installé
- [ ] Mes appareils sont à jour et scannés
- [ ] J'ai une sauvegarde récente de mes données importantes
- [ ] J'ai prévenu mon entourage du piratage
- [ ] J'ai déposé plainte si nécessaire

LE BON RÉFLEXE

Documentez tout

Dès la découverte du piratage, prenez des captures d'écran de tout ce que vous voyez : messages bizarres, transactions frauduleuses, emails de modification… Ces preuves seront indispensables pour le dépôt de plainte et le remboursement. Gardez-les dans un dossier dédié, classées par date.

SOS DESPY

Un piratage en cours ?

Le module SOS de votre espace Despy vous guide en temps réel selon votre situation. Plan d'action personnalisé en moins de 2 minutes.

QUIZ DE VALIDATION

Testez vos acquis

1 Premier réflexe quand vous découvrez que votre email est piraté ?

A Supprimer le compte immédiatement

B Changer le mot de passe depuis un autre appareil sûr

C Attendre 24h pour voir si ça s'arrange

2 Faut-il payer une rançon en cas de ransomware ?

A Oui, c'est le plus rapide

B JAMAIS — vous financez le crime sans garantie

C Seulement si la rançon est faible

3 **Quel numéro appeler en cas de violence numérique ?**

A Le 17

B Le 3018

C Le 15

4 **En cas de fraude bancaire, sous combien de temps la banque doit-elle vous rembourser ?**

A 30 jours

B 3 mois

C Selon le bon vouloir de la banque

5 **Quel site permet de trouver des outils gratuits de déchiffrement de ransomware ?**

A antivirus.fr

B nomoreransom.org

C police.gouv.fr

i RÉPONSES

Retrouvez les corrigés et le quiz interactif sur votre espace client Despy : **despy.fr** → Formation → Module 08.

09

MODULE 09 SUR 09

Arnaques par Intelligence Artificielle

L'IA a tout changé en 2026. Les escrocs l'utilisent pour écrire des messages parfaits, imiter la voix de vos proches et fabriquer de fausses vidéos. Voici comment garder une longueur d'avance.

À LA FIN DE CE MODULE, VOUS SAUREZ

- ✓ Reconnaître un email ou un SMS écrit par une IA
- ✓ Réagir face au clonage de voix au téléphone
- ✓ Repérer les faux sites et les fausses vidéos (deepfakes)
- ✓ Garder les bons réflexes, quelle que soit la menace

Pourquoi l'IA change la donne

Pendant des années, on répétait : « S'il y a des fautes d'orthographe, c'est une arnaque. » Ce réflexe ne marche plus. L'intelligence artificielle écrit aujourd'hui des messages parfaits, dans un français impeccable, et peut même imiter une voix ou un visage.

Le piège des messages parfaits

- Un email ou un SMS sans aucune faute n'est **plus du tout** une preuve de fiabilité.
- L'IA copie le ton et le vocabulaire de votre banque, des impôts ou de La Poste.
- Ce qui compte désormais : **le contenu** (on vous presse ? on demande des infos sensibles ?) et **l'adresse exacte** de l'expéditeur.

> ⚡ **LE RÉFLEXE QUI VOUS PROTÈGE**
>
> Ne jugez jamais un message à la qualité de son écriture. Vérifiez toujours **l'adresse après le @** et, au moindre doute, contactez l'organisme par son numéro officiel — jamais celui indiqué dans le message.

La voix de vos proches peut être clonée

- À partir de quelques secondes de voix (une vidéo, un message vocal), l'IA recrée une voix quasi identique.
- L'arnaque classique : « Maman, j'ai eu un accident, envoie-moi vite de l'argent. »
- La voix **n'est plus une preuve**. Raccrochez et rappelez la personne sur son numéro habituel.

Faux sites, deepfakes et fausses pubs

Des copies de sites parfaites

- L'IA recrée à l'identique le site de votre banque : logo, couleurs, mise en page.
- Le **cadenas** et le « https » ne prouvent rien : les sites d'arnaque en ont aussi.
- Seule **l'adresse exacte** compte. Méfiez-vous des variantes du type *labanque-securite.com*.
- Le plus sûr : tapez vous-même l'adresse, ou passez par votre application officielle.

Deepfakes : les fausses vidéos

- L'IA fabrique de fausses vidéos où une personnalité connue « recommande » un placement.
- Aucun placement sérieux n'est **garanti sans risque**. C'est le signal d'une arnaque.
- Vérifiez toute proposition d'investissement sur le registre officiel de l'AMF : **amf-france.org**.

✓ VOS 4 RÉFLEXES ANTI-IA

- ✓ Je ne me fie jamais à la qualité de l'écriture ni à la voix.
- ✓ Je vérifie l'adresse exacte (email et site web).
- ✓ Je ne clique pas dans l'urgence : je prends le temps de vérifier.
- ✓ En famille, on a convenu d'un **mot de passe secret** en cas de doute au téléphone.

QUIZ DE VALIDATION

Testez vos acquis

1 **Un email sans aucune faute d'orthographe prouve-t-il qu'il est fiable ?**

- **A** Oui, un escroc fait toujours des fautes
- **B** Non, l'IA écrit des messages parfaits : c'est le contenu qui compte
- **C** Oui, si le logo de la banque est présent

2 **Au téléphone, vous reconnaissez la voix de votre fils qui réclame de l'argent en urgence. Que faites-vous ?**

- **A** J'envoie l'argent, j'ai reconnu sa voix
- **B** Je raccroche et je le rappelle sur son vrai numéro
- **C** J'envoie une partie de la somme par prudence

3 **Un site identique à celui de votre banque s'affiche. Comment être sûr que c'est le vrai ?**

- **A** Si le design est parfait, c'est forcément le vrai
- **B** Je vérifie l'adresse exacte, ou je la tape moi-même
- **C** Je me fie au petit cadenas en haut

4 **Une vidéo montre une personnalité connue qui recommande un placement « garanti sans risque ». Que penser ?**

- **A** C'est fiable, c'est une personnalité connue
- **B** C'est très probablement un deepfake : une fausse vidéo générée par IA
- **C** Je teste avec une petite somme pour voir

5 **Un email « Meta for Business » annonce la suspension de votre compte sous 24h, avec un bouton. Bon premier réflexe ?**

- **A** Je clique vite pour ne pas perdre mon compte
- **B** Je regarde l'adresse de l'expéditeur : domaine inconnu = arnaque, je ne clique pas
- **C** Je réponds à l'email pour demander des explications

ℹ RÉPONSES

Retrouvez les corrigés et le quiz interactif sur votre espace client Despy : **despy.fr → Formation → Module 09**.

ANNEXE 1

Numéros et sites utiles à connaître

URGENCE (24h/24)

17	Police, gendarmerie
112	Numéro européen d'urgence

SIGNALEMENT

33700	Spam SMS, appels frauduleux
3018	Cyberharcèlement (gratuit, anonyme)

ASSISTANCE

0 805 805 817	Cybermalveillance.gouv.fr
116 006	France Victimes (aide gratuite)

OPPOSITION BANCAIRE

0 892 705 705	Opposition CB (interbancaire)

SITES À METTRE EN FAVORI

cybermalveillance.gouv.fr	Diagnostic + démarches
pharos.gouv.fr	Signaler un contenu illicite
signal-spam.fr	Signaler un email frauduleux
haveibeenpwned.com	Vérifier si votre email a fuité

PROTECTION QUOTIDIENNE

bloctel.gouv.fr	Liste anti-démarchage
pre-plainte-en-ligne.gouv.fr	Pré-plainte (gain de temps)
cnil.fr	Données personnelles, RGPD

ANNEXE 2

Glossaire
40 termes essentiels (1/2)

2FA / MFA
Double / multiple authentification. Étape de vérif en plus du mot de passe (SMS, app, clé).

Antivirus
Logiciel qui détecte et bloque les programmes malveillants (virus, ransomware, espions).

ANSSI
Agence nationale française de la sécurité des systèmes d'information.

Brouteur
Escroc qui simule une relation amoureuse pour soutirer de l'argent à sa victime.

Captcha
Test pour vérifier qu'un utilisateur est humain (cocher une case, identifier des images).

Chiffrement
Transformation d'une donnée en code illisible sans la clé. Protège la confidentialité.

Cookie
Petit fichier stocké par un site pour vous reconnaître ou suivre votre navigation.

Cybermalveillance
Plateforme publique d'aide aux victimes de cybermalveillance.gouv.fr.

Dark web
Partie d'Internet non indexée, où circulent données volées et trafics.

Deepfake
Vidéo, audio ou image truquée par IA, qui imite une personne réelle.

DNS
Annuaire d'Internet qui traduit un nom de site (exemple.fr) en adresse numérique.

Faille zero-day
Vulnérabilité d'un logiciel encore inconnue de l'éditeur, donc non corrigée.

Firewall
Pare-feu. Filtre les connexions entrantes et sortantes pour bloquer les intrus.

Gestionnaire MDP
Application qui génère et stocke vos mots de passe de manière sécurisée.

HIBP
Have I Been Pwned : service gratuit qui dit si votre email a fuité dans une faille.

HTTPS
Version sécurisée du protocole web. Cadenas visible dans la barre d'adresse.

Hameçonnage
Phishing en français. Email/SMS qui imite un site officiel pour voler vos identifiants.

Ingénierie sociale
Techniques de manipulation psychologique pour obtenir des informations confidentielles.

IoT
Objets connectés (montres, ampoules, caméras?) reliés à Internet.

Keylogger
Programme espion qui enregistre tout ce que vous tapez au clavier.

ANNEXE 2

Glossaire
40 termes essentiels (2/2)

Malware
Tout type de logiciel malveillant (virus, ransomware, cheval de Troie, espion).

MDP
Mot de passe. Doit être long, unique pour chaque compte et inattendu.

OTP
One-Time Password. Code à usage unique envoyé pour valider une connexion sensible.

Patch
Mise à jour qui corrige une faille de sécurité. À installer dès que possible.

PHAROS
Plateforme officielle pour signaler des contenus illicites en ligne (pédocriminalité, terrorisme?).

Phishing
Email frauduleux qui imite une marque connue pour vous piéger. Voir Hameçonnage.

Ransomware
Logiciel rançonneur qui chiffre vos fichiers et exige un paiement pour les déchiffrer.

RGPD
Règlement européen sur la protection des données personnelles depuis mai 2018.

Rootkit
Programme caché qui prend le contrôle de votre appareil sans être détecté.

Sextorsion
Chantage à la diffusion d'images intimes (vraies ou prétendues).

Skimming
Vol des données de carte bancaire via un faux dispositif sur un distributeur ou TPE.

Smishing
Phishing par SMS. Faux message de banque, livreur, opérateur, impôts?

Spam
Message non sollicité envoyé en masse, généralement publicitaire ou frauduleux.

Spear phishing
Phishing ciblé sur une personne précise, après recherches sur elle.

Spyware
Logiciel espion qui collecte vos données à votre insu (navigation, position, contacts).

SSL/TLS
Protocoles qui chiffrent les échanges entre votre navigateur et un site web.

Trojan
Cheval de Troie. Programme qui se cache dans une application apparemment légitime.

Usurpation
Le voleur utilise vos identifiants pour se faire passer pour vous.

Vishing
Phishing par téléphone. Faux conseiller bancaire, faux gendarme, faux technicien?

VPN
Réseau privé virtuel. Chiffre votre connexion et masque votre adresse IP.

MODÈLE DE LETTRE 1/3

Plainte au commissariat

À remettre au commissariat (ou en pré-plainte en ligne : pre-plainte-en-ligne.gouv.fr). Pensez à apporter vos pièces justificatives originales.

A envoyer a
Monsieur le Procureur de la République
Tribunal judiciaire de [votre ville]

Objet : Plainte contre X pour escroquerie en ligne

Madame, Monsieur,

Je soussigné(e) ..... porte plainte contre X pour les faits suivants :

Le ....., j'ai été victime de l'infraction suivante (cochez ce qui s'applique) :
[ ] Escroquerie sur Internet (article 313-1 du Code pénal)
[ ] Hameçonnage (phishing) ayant entraîné l'accès frauduleux à mes comptes
[ ] Usurpation d'identité numérique (article 226-4-1)
[ ] Piratage informatique (article 323-1)
[ ] Autre : .....

Préjudice subi : .....
Montant approximatif : ..... EUR

Je joins à cette plainte les éléments en ma possession (captures d'écran, emails, SMS, relevés bancaires, justificatifs d'achat?).

Je sollicite l'enregistrement de cette plainte et serai à disposition pour toute audition.

Je vous prie d'agréer, Madame, Monsieur, mes salutations distinguées.

Fait à ....., le .....
Signature : .....

MODÈLE DE LETTRE 2/3

Réclamation à votre banque

À envoyer en lettre recommandée avec accusé de réception. Conservez une copie. Votre banque doit vous rembourser sous 8 jours (loi).

A envoyer a
Service réclamations [Nom de votre banque]
Adresse de l'agence ou siège social

Objet : Contestation d'opérations non autorisées

Madame, Monsieur,

Titulaire du compte n° ..... dans votre établissement, je conteste formellement les opérations suivantes effectuées sans mon autorisation :

Date : ..... Montant : ..... EUR Bénéficiaire : .....
Date : ..... Montant : ..... EUR Bénéficiaire : .....

Conformément à l'article L133-18 du Code monétaire et financier, je sollicite le remboursement immédiat de ces opérations non autorisées.

J'ai immédiatement fait opposition à ma carte et déposé plainte auprès des services de police (récépissé joint).

Je vous remercie de me confirmer par écrit, sous 8 jours, la prise en charge de ma demande et le calendrier de remboursement.

Dans l'attente de votre retour, je vous prie d'agréer, Madame, Monsieur, mes salutations distinguées.

Fait à ....., le .....
Signature : .....

MODÈLE DE LETTRE 3/3

Demande d'effacement RGPD

À envoyer à toute entreprise détenant vos données (par email avec accusé de réception). Réponse obligatoire sous 1 mois.

A envoyer a

Délégué à la protection des données (DPO)
[Nom de l'entreprise]

Objet : Demande d'effacement de mes données personnelles (art. 17 RGPD)

Madame, Monsieur,

Conformément à l'article 17 du Règlement général sur la protection des données (RGPD), je vous demande l'effacement définitif de l'ensemble des données personnelles vous concernant me concernant et stockées par vos services :

Nom complet : .....
Adresse email : .....
Numéro de téléphone : .....
Identifiant client (si connu) : .....

Cette demande inclut toutes les sauvegardes, archives et copies, y compris celles détenues par vos sous-traitants.

Je vous rappelle que vous disposez d'un délai d'un mois pour répondre à ma demande (article 12 RGPD).

À défaut de réponse satisfaisante, je me réserve le droit de saisir la CNIL (Commission nationale de l'informatique et des libertés).

Fait à ....., le .....
Signature : .....

FICHE MEMO 1 / 6

J'ai perdu mon téléphone

Si votre téléphone a été perdu ou volé, agissez dans l'heure : vos comptes en banque, votre boîte email et vos applis y sont accessibles.

1. **Verrouillez-le à distance**

   iPhone : icloud.com/find. Android : android.com/find. Activez le mode « Perdu ».

2. **Bloquez votre carte SIM**

   Appelez votre opérateur pour suspendre la ligne. Cela empêche tout SMS d'arriver.

3. **Changez vos mots de passe critiques**

   Email principal d'abord, puis banque, puis comptes importants. Sur un autre appareil.

4. **Activez l'effacement à distance**

   Si vous ne retrouvez pas l'appareil dans les 24 h, effacez son contenu à distance.

5. **Déclarez la perte**

   Préfecture ou en ligne (service-public.fr). Conservez le récépissé pour votre opérateur.

CONSEIL DESPY

Activez « Localiser » avant qu'il ne soit trop tard. Sur iPhone : Réglages > Votre nom > Localiser. Sur Android : Paramètres > Sécurité > Localiser mon appareil.

FICHE MEMO 2 / 6

Ma carte bancaire est volée

Carte perdue, volée ou utilisée frauduleusement ? La loi vous protège, mais agissez vite : sous 13 mois maximum pour contester.

1. **Bloquez la carte immédiatement**

   Application bancaire (souvent en 1 clic), ou 0 892 705 705 (opposition interbancaire, 24h/24).

2. **Vérifiez les opérations récentes**

   Listez précisément date, montant, bénéficiaire de chaque débit frauduleux.

3. **Déposez plainte sous 24-48 h**

   Commissariat, gendarmerie, ou pré-plainte-en-ligne.gouv.fr. Conservez le récépissé.

4. **Contestez par écrit auprès de la banque**

   Lettre recommandée avec AR + copie de la plainte. Voir modèle dans les annexes.

5. **Demandez le remboursement**

   Article L133-18 : remboursement intégral sous 1 jour ouvré si vous n'êtes pas en faute.

CONSEIL DESPY

Si votre code PIN n'a pas été divulgué et que vous avez signalé la perte dans les 24h, votre responsabilité maximale est de 0 EUR.

FICHE MEMO 3 / 6

J'ai cliqué sur un lien suspect

Vous venez de cliquer sur un lien dans un email ou SMS douteux ? Voici les 5 réflexes pour limiter les dégâts dans l'heure.

1. **Coupez Wi-Fi et données mobiles**

   Mode Avion immédiatement. Cela bloque tout téléchargement en arrière-plan.

2. **Ne saisissez RIEN sur la page**

   Pas de mot de passe, pas d'email, pas de coordonnées bancaires, même si la page semble sûre.

3. **Changez vos mots de passe sensibles**

   Sur un AUTRE appareil sain : email principal, banque, puis tous les comptes liés.

4. **Scannez votre appareil**

   Antivirus à jour. Si vous suspectez un logiciel installé, faites une réinitialisation.

5. **Surveillez votre banque 30 jours**

   Activez les notifications sur chaque opération. Au moindre débit suspect : opposition.

CONSEIL DESPY

Le mode Avion ne suffit pas toujours. En cas de doute, contactez Despy via despy.fr/sos.

FICHE MEMO 4 / 6

Faux conseiller bancaire au téléphone

On vous appelle au nom de votre banque pour signaler une « opération suspecte » et vous demande votre code ? C'est une arnaque, dans 100 % des cas.

1. **Raccrochez IMMÉDIATEMENT**

   Ne discutez pas, ne donnez aucune information. Plus vous parlez, plus ils manipulent.

2. **Ne donnez JAMAIS de code reçu par SMS**

   Aucune banque ne demande votre code par téléphone. Ce code valide souvent un virement vers eux.

3. **Rappelez votre banque par le numéro officiel**

   Au dos de votre carte ou sur leur site officiel. Jamais le numéro qui vient de vous appeler.

4. **Signalez l'appel au 33700**

   Numéro officiel de signalement des arnaques téléphoniques. Gratuit, anonyme.

5. **Déposez plainte**

   Même si vous n'avez rien donné : ça aide la justice à remonter les filières. Récépissé à conserver.

CONSEIL DESPY

Phrase magique : « Je rappelle ma banque dans 5 minutes pour vérifier. » Aucun vrai conseiller ne refusera. Un arnaqueur, lui, insistera ou raccrochera.

FICHE MEMO 5 / 6

Réinitialiser mes comptes après piratage

Vous avez été piraté ? L'ordre dans lequel vous changez vos mots de passe est crucial. Suivez cette séquence à la lettre.

1. **L'email principal en PREMIER**

   C'est la clé de tous vos autres comptes (reset password). Mot de passe long, unique, et activez la 2FA.

2. **Activez la 2FA partout**

   Email, banque, réseaux sociaux, e-commerce. Préférez une application (Google Authenticator) au SMS.

3. **Vérifiez les connexions actives**

   Sur chaque compte : « Mes appareils » > déconnectez tout sauf le vôtre. Révoquez les apps tierces.

4. **Changez banque, RS, e-commerce**

   Dans cet ordre. Mots de passe TOUS différents, idéalement avec un gestionnaire (Bitwarden, 1Password).

5. **Surveillez le dark web**

   Inscrivez votre email sur haveibeenpwned.com pour être alerté en cas de nouvelle fuite.

CONSEIL DESPY

Despy fait ce travail pour vous : surveillance dark web continue, alerte en cas de fuite, et plan de réaction étape par étape. despy.fr

FICHE MEMO 6 / 6

Mon calendrier annuel de sécurité

Pour rester protégé toute l'année, voici 12 routines simples à faire 1 fois par mois. Cochez au fur et à mesure.

1

Janvier > Avril

Janv : change tes 3 mots de passe les plus critiques.
Fév : vérifie tes sauvegardes (photos, documents).
Mars : audit réseaux sociaux : qui te suit ?
Avril : nettoie les apps inutilisées du téléphone.

2

Mai > Août

Mai : scan dark web de tes emails (haveibeenpwned).
Juin : vérifie que la 2FA est active partout.
Juil : sauvegarde complète sur disque externe.
Août : vérifie tes consentements RGPD.

3

Septembre > Décembre

Sept : mets à jour ton système d'exploitation.
Oct : audit famille (parents, enfants).
Nov : prépare-toi aux arnaques de fêtes.
Déc : bilan annuel + bonnes résolutions cyber.

CONSEIL DESPY

Calendrier intégré dans votre espace despy.fr : un rappel par mois, une routine, un score qui grimpe. Sans effort.

FELICITATIONS

Vous l'avez fait.

Vous venez de boucler les **9** modules essentiels de la cybersécurité pour particuliers.

VOUS SAVEZ MAINTENANT

- ✓ Reconnaître un email frauduleux
- ✓ Déjouer les arnaques par SMS
- ✓ Créer des mots de passe inattaquables
- ✓ Activer la double authentification
- ✓ Protéger vos appareils au quotidien
- ✓ Acheter en ligne sans tomber dans les pièges
- ✓ Sécuriser vos réseaux sociaux
- ✓ Réagir efficacement en cas de piratage

Mais en cybersécurité, les arnaques évoluent chaque jour. Restez équipé toute l'année.

Continuez votre protection sur despy.fr

Conseiller IA 24h/24 · Alertes en temps réel · Surveillance dark web · Centre SOS d'urgence · Formation continue

Activez votre protection : 9,99 EUR/mois, sans engagement.

06 89 14 83 95
Strasbourg, France