



fem-mias

WOMEN IN MICRO-BUSINESSES
ASK FOR SUSTAINABLE GROWTH

Training programme for micro-business management

Module 3: Growing your business through digital

Name:

*Digital Skills
training*



Project's ID

Date de début: 01/09/2024

Date de fin: 31/03/2026

Durée totale: 19 mois

4 objectifs:

- Soutenir la croissance et la pérennité des microentreprises dirigées par des femmes (+3 ans)
- Donner aux femmes ciblées les moyens de développer une microentreprise durable
- Échanger des pratiques et faciliter les échanges de connaissances transfrontaliers
- Renforcer les capacités des partenaires à mieux accompagner le public cible



Public cible du projet



Des femmes, quel que soit leur âge,
dirigeant une micro-entreprise depuis au
moins 3 ans.

Elles souhaitent pérenniser leur activité
et en vivre décemment.



Project's partners

Mompreneurs asbl

L'ASBL des Mompreneurs de Belgique est un réseau d'environ 200 membres. Fondé en 2011, il soutient les mamans entrepreneurs, et promeut la solidarité, l'équilibre et l'épanouissement par le biais d'événements, de formations et de réseautage.



Mulheres a Obra

Mulheres à Obra est le plus grand réseau d'entrepreneuriat féminin du Portugal, avec plus de 180 000 membres. Fondé en 2017, il accompagne les femmes dans leur développement grâce à des formations, du réseautage et des projets collaboratifs.



IKF Malmö

IKF Malmö est une organisation à but non lucratif qui soutient les femmes nées à l'étranger depuis 1970. Elle propose des cours de langues, des formations et des événements pour promouvoir l'inclusion, l'égalité et l'autonomisation des femmes d'horizons divers.





Project's activities



*A1 –
Développement
d'une nouvelle
série de formations
pour soutenir la
croissance durable
des
microentreprises
dirigées par des
femmes*



*A2 – Test et mise
en œuvre de la
nouvelle série de
formations*



*A3 – Activités de
communication :
toucher les femmes
entrepreneures à la
tête d'une micro-
entreprise*



*A4 – Phase
d'évaluation
du programme
de formations*



*A5 –
Conférence de
diffusion et
activité de
cloture du
projet*



Save-the- dates

Les prochaines activités du projet FEM-MIAS:

- *Le vendredi 21 novembre 2025 de 9h30 à midi:*
En ligne et gratuit
BOOTCAMP regroupant les participantes aux formations dans les 3 pays – partages d'expérience et échanges avec d'autres entrepreneurs d'horizons différents
- *Le jeudi 29 Janvier 2026 à 17h*
à Bruxelles (lieu à confirmer) et gratuit
CONFÉRENCE et ÉVÉNEMENT de clôture du projet en présence des partenaires



Cyber security

*Protéger son activité digitale sans devenir
parano*

Atelier de sensibilisation



Cybersécurité, kezaco?

Quand vous entendez le mot cybersécurité, à quoi pensez-vous ?

- A. À des hackers en sweat à capuche dans le noir, pas vraiment à vous !
- B. À des mots de passe, des arnaques par mail et quelques trucs à surveiller...
- C. À une stratégie que vous avez déjà mise en place pour protéger votre business.



Et si vous étiez une hackeuse ?

 Si vous vouliez pirater une entrepreneure comme vous, comment feriez-vous ?

- Faux mails (phishing) ?
- Mot de passe deviné ?
- Faux client ou fausse facture ?
- Récupération de données via un wifi public ?

Penser comme une hackeuse permet de détecter vos propres failles !



L'Evil Twin

Quelqu'un vole votre identité professionnelle en ligne. Que faites-vous ?

- Signaler le faux compte à la plateforme
- Alerter vos clients
- Changer tous vos mots de passe
- Vérifier vos fuites de données
- Protéger votre nom de domaine et vos marques



Votre image de marque est un actif précieux à sécuriser



La Valeur de vos données

Combien valent vos identifiants sur le dark web ?

Email perso : 1 à 10 €

Email pro / PayPal : 100 €

Accès bancaire : 1000 €+

 Testez sur : www.haveibeenpwned.com



Vos données sont une monnaie d'échange.



Votre sac à main (ou à dos)

Et si quelqu'un vole votre sac ?



Listez 5 objets sensibles dans votre sac



Puis 5 actifs numériques en cas de piratage (ex : fichiers clients, accès bancaire...)

Comparez : vous protégez mieux vos objets que vos données ?



Votre laptop vaut – sans doute - plus que votre sac à main !



La cybersécurité est une alliée

1. Elle protège vos revenus
2. Moins de stress numérique
3. Votre identité digitale = un actif
4. Sécurise les collaborations à distance
5. Money loves security !



Le terrain de jeu préféré des hackers

Vos mots de passe !

Exercice express: noter un mot de passe que vous pourriez choisir

Est-il suffisamment safe?

- ✓ 12 caractères mini
- ✓ Pas de données personnelles
- ✓ Pas réutilisé
- ✓ Passphrase unique (ex : Soleil@Plage2024!)



Qui a les clés ?

Listez vos 5 comptes clés

Check:

- Qui y a accès ?
- L'authentification 2FA est-elle active ?
- Ancien(s) collaborateur(s) ou autre(s) toujours connecté(s) ?
- Y a-t-il une adresse e-mail de recuperation ?



Phishing: ne mordez pas à l'hameçon

3 signaux d'alerte dans les e-mails suspects:

1. Nom de domaine étrange (ex : @paypal-secure.com)
2. Ton urgent / menaçant
3. Lien bizarre ou raccourci

Règle des 3 vérifications :

1. Je survole les liens
2. Je ne clique pas dans le doute
3. Je vérifie à la source (appel, recherche directe)



Créer son plan d'urgence

1. Restez calme
2. Changez vos mots de passe
3. Informez vos abonnés/clients
4. Scannez votre appareil
5. Contactez la plateforme concernée
6. Activez le 2FA partout

 Préparez un plan en 3 étapes + 3 contacts de confiance



5 bons réflexes

1. Activez le 2FA sur 1 compte critique
2. Changez un mot de passe faible
3. Révoquez un accès inutile (ancien prestataire)
4. Sauvegardez un dossier important sur le cloud
5. Vérifiez vos fuites de données (haveibeenpwned.com)



Challenge : cochez-en 3 pendant cette semaine !



Les outils

Outils recommandés :

- Gestion de mots de passe : Bitwarden / 1Password / Apple...
- Scans d'emails suspects : www.virustotal.com
- Sauvegarde : Google Drive / Dropbox
- Check : www.haveibeenpwned.com
- Dénoncer les mails suspects: suspect@safeonweb.be



Training Programme For Leader Women in Europe Family Businesses