

Fiche Pratique N°40 : Sécurisez votre BIOS/UEFI – La première porte d'entrée de votre ordinateur V1.0

Objectif : Comprendre les enjeux de souveraineté du BIOS/UEFI, faire un choix éclairé concernant Secure Boot, et sécuriser le démarrage de votre ordinateur sans dépendre inutilement de Microsoft.

•**Public visé :** Intermédiaire à Avancé (utilisateurs Linux, militants, exigeants sur la souveraineté numérique)

•**Temps estimé :** 20 à 40 minutes (lecture + configuration)

•**Niveau de difficulté :** ★★★☆☆ (Moyen)

Prérequis : Savoir redémarrer votre ordinateur. Savoir accéder au BIOS/UEFI (voir tableau des touches dans la fiche plus bas). Avoir un ordinateur sous Linux pour les commandes avancées (optionnel).

Pour qui est cette fiche ?

-
- ☒ Vous installez Linux sur un PC récent (Secure Boot peut bloquer l'installation)
 - ☒ Vous voulez comprendre la dépendance à Microsoft via Secure Boot
 - ☒ Vous êtes militant / journaliste et voulez éviter les puces d'espionnage (Intel ME / AMD PSP)
 - ☒ Vous êtes exigeant sur la souveraineté numérique
-

Le problème en une minute

Problème	Explication
Secure Boot	Protège contre les logiciels malveillants au démarrage... mais les clés par défaut sont celles de Microsoft.
Dépendance à Microsoft	Linux ne peut démarrer avec Secure Boot activé que grâce à SHIM, un programme signé par Microsoft.

Fiche Pratique N°40 : Sécurisez votre BIOS/UEFI – La première porte d'entrée de votre ordinateur V1.0

Problème	Explication
Intel ME / AMD PSP	Des puces intégrées aux processeurs modernes avec un accès privilégié (potentielles backdoors).
TPM	Une puce « coffre-fort » rendue obligatoire par Windows 11 (mais utile aussi sous Linux).

La décision clé : Sur un PC Linux uniquement, **désactiver Secure Boot** est la décision la plus souveraine.

Table des matières

1. BIOS vs UEFI : rappels.....	3
2. Le problème de fond : Secure Boot renforce-t-il notre dépendance à Microsoft ?.....	3
3. La puce d'espionnage : Intel Management Engine (ME) et AMD Platform Security Processor (PSP).....	4
Pourquoi c'est un problème pour votre souveraineté numérique.....	5
Que faire face à Intel ME / AMD PSP ?.....	5
Recommandations par profil.....	6
4. Vos choix stratégiques concernant Secure Boot (à faire MAINTENANT).....	6
Recommandations par profil (Secure Boot).....	7
5. Comment désactiver Secure Boot (étape par étape).....	8
6. Détails techniques (si besoin d'un dual boot Linux / Windows 11).....	8
6.1 Comment Secure Boot fonctionne avec Linux (si activé).....	8
6.2 Distributions Linux compatibles avec Secure Boot.....	9
6.3 Vérifier l'état de Secure Boot sous Linux.....	9
6.4 Gérer ses propres clés (MOK) – pour les experts.....	10
6.5 Les modules noyau et Secure Boot.....	10
6.6 Le TPM (Trusted Platform Module).....	11
6.7 Le TPM et la dépendance à Microsoft.....	11
7. Autres réglages de sécurité (indépendants de Secure Boot).....	12
Mise à jour du BIOS sous Linux (fwupdmgrr).....	12
8. Vérifier le mode (BIOS ou UEFI) et GRUB sous Linux.....	13
Vérifier le mode.....	13
GRUB (chargeur de démarrage Linux).....	13
9. Cas spécifiques à Linux (Mint, Ubuntu, etc.).....	14
10. Comment accéder au BIOS ? (touches par marque).....	14
11. Tableau récapitulatif des options (Secure Boot).....	15
12. Challenge 7 jours.....	16
13. En résumé – ce que vous gagnez.....	16
14. Conclusion générale.....	16
Test final :.....	17

Fiche Pratique N°40 : Sécurisez votre BIOS/UEFI – La première porte d'entrée de votre ordinateur V1.0

1. BIOS vs UEFI : rappels

Caractéristique	BIOS (Legacy)	UEFI
Époque	Années 1980 (obsolète)	Moderne (depuis 2010)
Interface	Écran bleu, clavier uniquement	Graphique (parfois souris)
Démarrage	Lent	Rapide
Disques	Limitée à MBR ≤ 2 To	Gère les disques récents GPT > 2 To
Sécurité	Aucune	Secure Boot, TPM

Ce qu'ils font : C'est le tout premier programme qui s'exécute quand vous allumez votre ordinateur, avant le système d'exploitation (Windows, Linux, macOS). Négliger sa sécurité, c'est laisser la porte d'entrée grande ouverte.

2. Le problème de fond : Secure Boot renforce-t-il notre dépendance à Microsoft ?

Secure Boot est censé protéger contre les logiciels malveillants qui s'exécutent avant le système d'exploitation. Mais **qui contrôle les clés ?**

Point clé	Explication
Les clés par défaut sont celles de Microsoft	Quand vous achetez un PC, le firmware UEFI contient uniquement les clés publiques de Microsoft (et parfois celle de quelques fabricants). Sans ces clés, aucun système ne pourrait démarrer.
Linux dépend d'un programme signé par Microsoft (SHIM)	Pour que Linux puisse démarrer avec Secure Boot activé, un petit programme appelé SHIM doit être signé par... Microsoft. SHIM fait le pont entre le monde Microsoft et le monde Linux.

Fiche Pratique N°40 : Sécurisez votre BIOS/UEFI – La première porte d'entrée de votre ordinateur V1.0

Point clé	Explication
Microsoft peut théoriquement révoquer cette signature	Si Microsoft décidait de révoquer la signature de SHIM (pour une raison quelconque), des millions de PC Linux ne pourraient plus démarrer.
Windows 11 exige Secure Boot + TPM 2.0	C'est une façon délibérée de rendre l'installation de Linux plus complexe sur du matériel neuf (même si techniquement possible).

En clair : Secure Boot, tel qu'il est implémenté sur la quasi-totalité des PC grand public, **verrouille le marché autour de Microsoft**. Ce n'est pas une fatalité, mais il faut en être conscient.

3. La puce d'espionnage : Intel Management Engine (ME) et AMD Platform Security Processor (PSP)

Au-delà de Secure Boot, un autre problème de souveraineté se pose : **tous les processeurs modernes (Intel et AMD) contiennent une puce intégrée qui a un accès privilégié et permanent à votre matériel**.

Puce	Fabricant	Depuis	Rôle théorique	Problème
Intel Management Engine (ME)	Intel	2008	Gestion à distance, maintenance	Accès indépendant au réseau, à la mémoire, au clavier. Peut être activé même ordinateur éteint.
AMD Platform Security Processor (PSP)	AMD	2013	Équivalent de l'Intel ME	Mêmes capacités d'accès privilégié.

Fiche Pratique N°40 : Sécurisez votre BIOS/UEFI – La première porte d'entrée de votre ordinateur V1.0

Pourquoi c'est un problème pour votre souveraineté numérique

Capacité	Risque
Accès indépendant au réseau	La puce peut communiquer sur Internet sans que vous le sachiez, même ordinateur éteint (via Wake-on-LAN).
Accès à la mémoire vive	Peut lire ce que vous faites (frappes au clavier, mots de passe, documents ouverts).
Accès aux périphériques	Peut intercepter ce qui passe par le clavier, la souris, le disque dur.
Impossible à désactiver complètement	Sur les PC récents, Intel ME est de plus en plus difficile à neutraliser.


Que faire face à Intel ME / AMD PSP ?

Solution	Efficacité	Difficulté	Compatibilité
Ignorer (usage domestique standard)	Faible (vous acceptez le risque)	★☆☆☆☆	Tous les PC
Désactiver partiellement (via BIOS)	Certains paramètres BIOS peuvent limiter (mais pas supprimer)	★★★☆☆	Certains PC (rare)
me_cleaner (supprime une partie du code)	Partielle (réduit les fonctionnalités, mais ne supprime pas tout)	★★★★★	Certains ThinkPad, Purism, System76
Acheter du matériel sans ME/PSP	Totale	★★★☆☆ (achat)	Purism Librem, System76 (partiellement), vieux PC antérieur à 2008
Utiliser un firmware libre (Libreboot / Coreboot)	Totale (avec matériel compatible)	★★★★★	Matériel limité (ThinkPad X200, T400, etc.)

Fiche Pratique N°40 : Sécurisez votre BIOS/UEFI – La première porte d'entrée de votre ordinateur V1.0


Recommandations par profil

Profil	Que faire face à Intel ME / AMD PSP ?
Utilisateur domestique	Ignorez. Le risque est théorique pour un particulier. Concentrez-vous sur les autres sécurités (mots de passe, 2FA, sauvegardes).
Exigeant / paranoïaque	Choisissez un PC compatible <code>me_cleaner</code> (certains ThinkPad). Appliquez <code>me_cleaner</code> (opération avancée).
Journaliste / militant	Achetez un Purism Librem (Intel ME désactivé en usine) ou un System76 (réduction partielle).
Puriste du logiciel libre	Utilisez un firmware Libreboot sur matériel compatible (ThinkPad X200, T400).

 **À savoir** : Sur les PC grand public récents (2020+), il est devenu très difficile, voire impossible, de désactiver complètement l'Intel ME. Les fabricants verrouillent les accès. La seule solution fiable est d'acheter du matériel spécialisé.

4. Vos choix stratégiques concernant Secure Boot (à faire MAINTENANT)

Avant même d'entrer dans les détails techniques, voici les options qui s'offrent à vous.

Choix	Dépendance à Microsoft	Niveau technique	Recommandation
1. Désactiver Secure Boot (recommandé pour Linux seul)	 Aucune	★☆☆☆☆ (simple)	Idéal pour la souveraineté
2. Garder Secure Boot avec SHIM (solution par défaut)	 Oui (indirecte)	★☆☆☆☆ (simple)	Acceptable pour dual boot Windows 11
3. Ajouter ses propres clés	 Partielle (clés)	★★★★★	Pour les experts

Fiche Pratique N°40 : Sécurisez votre BIOS/UEFI – La première porte d'entrée de votre ordinateur V1.0

Choix	Dépendance à Microsoft	Niveau technique	Recommandation
(MOK)	Microsoft restent)	(avancé)	seulement
4. Remplacer les clés par défaut	✗ Aucune	★★★★★ (très avancé)	Risqué, réservé aux experts
5. Acheter du matériel avec clés Linux intégrées	✗ Aucune	★★★☆☆ (aucune config)	Idéal pour un nouveau PC
6. Utiliser un firmware libre (Coreboot/Libreboot)	✗ Aucune	★★★★★ (très avancé)	Pour passionnés, matériel limité

Recommandations par profil (Secure Boot)

Profil	Ce que je vous conseille
Linux seul (grand public)	Désactivez Secure Boot. Point final. Vous ne perdez quasiment rien en sécurité, et vous gagnez en indépendance.
Linux seul (exigeant, nouveau PC)	Achetez un ordinateur Purism, System76 ou Tuxedo . Ils intègrent leurs propres clés (ou permettent une désactivation propre).
Dual boot Linux + Windows 11	Vous n'avez pas le choix : laissez Secure Boot activé (Windows 11 l'exige). Acceptez la dépendance à Microsoft.
Journaliste / militant (anonymat)	Désactivez Secure Boot (Tails le désactive volontairement).
Puriste du logiciel libre	Utilisez un firmware libre (Libreboot) sur du matériel compatible (ThinkPad X200, T400, etc.).

💡 **Si vous hésitez encore** : La désactivation de Secure Boot sur un PC Linux uniquement n'a quasiment aucun inconvénient pratique. C'est la décision la plus souveraine.

5. Comment désactiver Secure Boot (étape par étape)

Si vous avez choisi l'option 1 (recommandée pour Linux seul) :

- 1.Redémarrez l'ordinateur.
- 2.Entrez dans le BIOS/UEFI (voir tableau des touches §10).
- 3.Allez dans l'onglet Boot ou Security.
- 4.Trouvez l'option Secure Boot.
- 5.Passez à Disabled.
- 6.Sauvegardez et quittez (généralement F10).

C'est fini. Plus aucune dépendance à Microsoft pour le démarrage.

6. Détails techniques (si besoin d'un dual boot Linux / Windows 11)

Cette section n'est utile que si vous avez choisi de garder Secure Boot activé (dual boot avec Windows 11) ou si vous êtes curieux.

6.1 Comment Secure Boot fonctionne avec Linux (si activé)

La chaîne de confiance :

UEFI (firmware)

|

▼ (vérifie la signature de SHIM)

| SHIM (petit programme signé par Microsoft) |

| - SHIM est le seul composant Linux signé par Microsoft |

| - Il fait le pont entre le monde Microsoft et le monde Linux |

|

▼ (SHIM vérifie la signature de GRUB)

Fiche Pratique N°40 : Sécurisez votre BIOS/UEFI – La première porte d'entrée de votre ordinateur V1.0

GRUB (chargeur de démarrage)	
- GRUB peut être signé par SHIM ou par une clé MOK	
▼ (GRUB vérifie la signature du noyau)	
Noyau Linux (vmlinuz)	

SHIM est le seul composant Linux signé par Microsoft. Sans lui, pas de Linux avec Secure Boot activé.

6.2 Distributions Linux compatibles avec Secure Boot

Distribution	Compatible ?	Remarque
Ubuntu, Fedora, Mint (21.2+), Debian 11+	✓ Oui	SHIM intégré, installation immédiate
Arch, Manjaro, Gentoo	⚠ Partielle	Configuration manuelle requise
Tails	✗ Non (volontaire)	Désactive Secure Boot par conception

6.3 Vérifier l'état de Secure Boot sous Linux

Méthode 1 : avec mokutil (recommandé)

```
mokutil --sb-state
```

SecureBoot enabled (activé) / disabled (désactivé)

Méthode 2 : autre façon

```
cat /proc/sys/kernel/secureboot
```

0 = désactivé, 1 = activé

Méthode 3 : dans les logs du noyau

```
dmesg | grep -i secure
```

6.4 Gérer ses propres clés (MOK) – pour les experts

MOK (Machine Owner Key) permet d'ajouter vos propres clés de signature sans modifier le BIOS.

Cas d'usage typiques : pilote NVIDIA non signé, compilation de votre propre noyau, module noyau tiers (VirtualBox, etc.).

Ajouter sa propre clé

```
sudo mokutil --import /chemin/vers/ma_cle.der
```

Redémarrer (un écran bleu MOK apparaît au démarrage)

Suivre les instructions, saisir le mot de passe, choisir "Enroll key"

```
sudo reboot
```

Lister les clés

```
sudo mokutil --list-enrolled
```

Supprimer une clé

```
sudo mokutil --delete /chemin/vers/ma_cle.der
```

```
sudo reboot
```

6.5 Les modules noyau et Secure Boot

Le noyau Linux vérifie la signature des modules (pilotes) qu'il charge.

Vérifier qu'un module est signé

```
modinfo nom_du_module | grep -i signature
```

Si le module n'est pas signé : dmesg affiche "module verification failed"

Solution





Niveau

Désactiver Secure Boot (recommandé pour Linux seul)	★☆☆☆☆
---	-------

Signer le module avec MOK	★★★★★
---------------------------	-------

6.6 Le TPM (Trusted Platform Module)

Le TPM est une puce (ou module firmware) soudée à la carte mère servant de **coffre-fort matériel** pour les clés de chiffrement.

Fonction	Explication
 Stockage sécurisé de clés	Mots de passe, certificats
 Chiffrement des données	Utilisé par BitLocker (Windows), LUKS + Clevis (Linux)
 Démarrage sécurisé	Renforce Secure Boot
 Authentification	Windows Hello, etc.

Sous Linux :

```
ls /dev/tpm*  
sudo dmesg | grep -i tpm  
tpm2_pcrread    # si tpm2-tools installé
```

Sous Windows : tpm.msc

| Windows 11 exige TPM 2.0 + Secure Boot + UEFI.

6.7 Le TPM et la dépendance à Microsoft

Le TPM en lui-même n'est pas une technologie Microsoft – c'est une norme ouverte (ISO/IEC 11889) définie par le Trusted Computing Group. **Mais Microsoft a rendu le TPM obligatoire** en l'exigeant pour Windows 11. Tous les PC neufs depuis 2021 sont donc équipés d'un TPM (souvent soudé à la carte mère).

Sous Linux, le TPM n'est pas nécessaire. Vous pouvez l'ignorer ou l'utiliser librement avec des outils comme `systemd-cryptenroll` (sans dépendre de Microsoft). Si vous voulez éviter totalement le TPM, achetez un PC antérieur à 2016 ou une marque spécialisée (Purism, System76) qui permet de le désactiver matériellement.

Fiche Pratique N°40 : Sécurisez votre BIOS/UEFI – La première porte d'entrée de votre ordinateur V1.0

7. Autres réglages de sécurité (indépendants de Secure Boot)

Action	Où la trouver (dans le BIOS)	Pourquoi
✓ Mettre à jour le firmware	Site fabricant ou fwupdmgr	Corrige les failles de sécurité
✓ Définir un mot de passe administrateur	Security → Set Administrator Password	Empêche les modifications non autorisées
✓ Désactiver le boot sur USB/DVD	Boot → Boot Order	Empêche le démarrage sur périphérique malveillant
✓ Désactiver le boot sur réseau (PXE)	Boot → Network Boot → Disable	Évite le démarrage sur serveur distant
✓ Désactiver Thunderbolt (si inutilisé)	Peripherals → Thunderbolt → Disable	Réduit la surface d'attaque
✓ Activer TPM (si disponible)	Security → TPM → Enable	Renforce le chiffrement

Mise à jour du BIOS sous Linux (fwupdmgr)

De nombreux fabricants (Dell, Lenovo, HP, System76) publient les mises à jour firmware sur le **LVFS** :

```
fwupdmgr get-devices    # Voir les périphériques compatibles
```

```
fwupdmgr refresh        # Rafraîchir la liste des mises à jour
```

```
fwupdmgr get-updates    # Voir les mises à jour disponibles
```

```
sudo fwupdmgr update    # Appliquer les mises à jour
```

Tous les PC ne sont pas compatibles. Si fwupdmgr ne trouve rien, vérifiez sur le site du fabricant.

8. Vérifier le mode (BIOS ou UEFI) et GRUB sous Linux

Vérifier le mode

Méthode 1 : vérifier l'existence du dossier efi

```
ls /sys/firmware/efi
```

```
[ -d /sys/firmware/efi ] && echo "UEFI" || echo "BIOS"
```

Méthode 2 : vérifier la partition EFI

```
lsblk -f # chercher partition vfat/FAT32 sur /boot/efi
```

Méthode 3 : utiliser efibootmgr

```
sudo efibootmgr # si commande existe, vous êtes en UEFI
```

GRUB (chargeur de démarrage Linux)

Accès au menu GRUB au démarrage :

- Mode BIOS (Legacy) : maintenir la touche **Shift** enfoncée
- Mode UEFI : appuyer plusieurs fois sur la touche **Esc**

Modifier le temps d'affichage du menu GRUB :

```
sudo nano /etc/default/grub
```

Modifier les lignes :

```
GRUB_TIMEOUT_STYLE=hidden → GRUB_TIMEOUT_STYLE=menu  
GRUB_TIMEOUT=5
```

Puis :

```
sudo update-grub
```

9. Cas spécifiques à Linux (Mint, Ubuntu, etc.)

Situation	Action recommandée
Installation impossible (erreur "Secure Boot violation")	Désactivez Secure Boot dans le BIOS (ou activez le mode "Other OS").
Démarrage sur clé USB après installation	Remettez le disque dur interne en première position dans l'ordre de boot.
Mot de passe BIOS perdu	Essayez de vider le CMOS (retirer la pile quelques minutes). Sinon, contactez le fabricant.
Ajouter ses propres clés Secure Boot	Utilisez <code>mokutil --import</code> pour ajouter une clé MOK.
NVIDIA / VirtualBox ne fonctionnent pas	Soit désactivez Secure Boot, soit signez les modules avec MOK.

10. Comment accéder au BIOS ? (touches par marque)

Marque	Touche(s)	Remarque
Acer	F2 ou Suppr (Del)	Ctrl+S active des options cachées
Apple (Mac Intel)	Option + Commande + P + R	Mac M1/M2 : pas de BIOS traditionnel
Asus	F2 ou Suppr	PC fixes souvent Suppr, portables F2
Dell	F2	F12 = menu boot
HP	F10 ou Esc	Esc → menu, puis F10
Lenovo (ThinkPad)	F1 ou F2	Certains : Entrée puis F1
Lenovo (IdeaPad)	F2 ou Fn+F2	—
MSI	Suppr (Del)	—
PC assemblé	Suppr (Del) ou F2	—

Fiche Pratique N°40 : Sécurisez votre BIOS/UEFI – La première porte d'entrée de votre ordinateur V1.0

Marque	Touche(s)	Remarque
Microsoft Surface	Volume + (longue pression)	—

Méthode universelle : Appuyez plusieurs fois sur F2, F10, F12, Suppr ou Esc dès que l'ordinateur démarre.

Depuis Windows : Paramètres → Mise à jour et sécurité → Récupération → Démarrage avancé → Redémarrer maintenant → Dépannage → Options avancées → Paramètres du firmware UEFI → Redémarrer.

11. Tableau récapitulatif des options (Secure Boot)

Option	Dépendance à Microsoft	Sécurité	Difficulté	Recommandation
Désactiver Secure Boot	 Aucune	★ ★ ☆ ☆ ☆	★ ☆ ☆ ☆ ☆	Pour Linux seul
Garder Secure Boot + SHIM	 Oui	★ ★ ★ ★ ★	★ ☆ ☆ ☆ ☆	Dual boot Windows 11
Ajouter clés MOK	 Partielle	★ ★ ★ ★ ★	★ ★ ★ ★ ★	Experts
Remplacer clés par défaut	 Aucune	★ ★ ★ ★ ★	★ ★ ★ ★ ★ ★	Très avancé
Matériel avec clés Linux	 Aucune	★ ★ ★ ★ ★	★ ★ ★ ☆ ☆ ☆	Nouveau PC
Firmware libre	 Aucune	★ ★ ★ ★ ★ ★	★ ★ ★ ★ ★ ★	Passionnés

12. Challenge 7 jours

Jour 1 : Identifiez la touche d'accès au BIOS. Entrez dans le BIOS.

Jour 2 : Vérifiez la version du firmware. Cherchez une mise à jour (site fabricant ou fwupdmgr).

Jour 3 : Définissez un mot de passe administrateur (stockez-le dans Bitwarden).

Jour 4 : Désactivez le boot sur USB/DVD.

Jour 5 : Activez TPM (si disponible).

Jour 6 : Prenez votre décision concernant Secure Boot (désactivez-le si Linux seul, laissez-le si dual boot Windows 11).

Jour 7 : Redémarrez. Vérifiez que tout fonctionne.

13. En résumé – ce que vous gagnez

Action	Gagné
Désactiver Secure Boot (Linux seul) Indépendance totale vis-à-vis de Microsoft	
Acheter un PC Purism / System76 / Tuxedo	Matériel respectueux, pas de dépendance, Intel ME désactivé
Mettre à jour le firmware	Sécurité matérielle (failles corrigées)
Mot de passe BIOS + désactiver boot USB	Protection contre les accès physiques non autorisés
Utiliser me_cleaner (experts)	Réduction de la surface d'attaque Intel ME

14. Conclusion générale

Profil	Décision Secure Boot	Décision Intel ME / PSP
Linux seul (grand public)	Désactivez Secure Boot	Ignorez (risque faible)
Linux seul (exigeant,	Achetez du matériel avec clés	Achetez Purism / System76

Fiche Pratique N°40 : Sécurisez votre BIOS/UEFI – La première porte d'entrée de votre ordinateur V1.0

Profil	Décision Secure Boot	Décision Intel ME / PSP
nouveau PC)	Linux	
Dual boot Linux + Windows 11	Laissez Secure Boot activé (obligatoire)	Ignorez (ou achetez matériel compatible)
Journaliste / militant	Désactivez Secure Boot	Achetez Purism Librem
Puriste / militant du libre	Firmware libre (Libreboot)	Firmware libre (Libreboot)

À retenir absolument :

- **Secure Boot, sur PC grand public, renforce la dépendance à Microsoft.** C'est un fait technique.
- **Sur Linux seul, désactiver Secure Boot est la décision la plus souveraine.**
- **Windows 11 vous oblige à garder Secure Boot activé** – c'est un choix à faire en connaissance de cause.
- **Intel ME / AMD PSP sont des puces d'espionnage potentielles.** Sur les PC récents, il est devenu très difficile de les désactiver. Seules des marques spécialisées (Purism, System76) le permettent vraiment.
- **Des alternatives matérielles existent** (Purism, System76, Tuxedo) pour ceux qui veulent la sécurité **et** l'indépendance.
- **Notez votre mot de passe BIOS** dans Bitwarden (fiche N°16) – sans lui, vous ne pourrez plus modifier la configuration.

Test final :

1. ☒ J'ai compris que Secure Boot, sur PC grand public, renforce la dépendance à Microsoft.
2. ☒ Je sais que les processeurs récents contiennent une puce (Intel ME / AMD PSP) avec accès privilégié.
3. ☒ J'ai fait un choix éclairé concernant Secure Boot (désactivé si Linux seul, activé si dual boot Windows 11).
4. ☒ J'ai défini un mot de passe administrateur BIOS.

Fiche Pratique N°40 : Sécurisez votre BIOS/UEFI – La première porte d'entrée de votre ordinateur V1.0

5. ☒ J'ai désactivé le boot sur USB/DVD.
6. ☒ J'ai vérifié la version de mon firmware (et l'ai mise à jour si nécessaire).
7. ☒ Mon ordinateur démarre normalement.

Félicitations ! Vous avez repris le contrôle de la première couche logicielle de votre ordinateur, et vous êtes conscient des enjeux de souveraineté.

Ressources :

- `me_cleaner` : https://github.com/corna/me_cleaner
- `fwupdmgr` (mises à jour firmware) : <https://fwupd.org>
- `mokutil` : gestion des clés Secure Boot sous Linux
- **Purism** (PC sans Intel ME) : <https://puri.sm>
- **System76** : <https://system76.com>
- **Tuxedo Computers** (européen) : <https://www.tuxedocomputers.com>
- **Libreboot** (firmware libre) : <https://libreboot.org>
- Liste des PC compatibles avec la désactivation Intel ME : <https://hardware-libre.fr>