Des Solutions des sécurités existes.

Je vais vous donner comme exemple la solution de sécurité mise en place au collège Saint joseph depuis plus de 10 ans. (Deep Freeze)

La problématique.

Certains professeurs qui croyaient connaitre suffisamment l'informatique modifiaient ou laissaient les élèves modifier les ordinateurs pendant leurs cours.

Le professeur suivant qui voulait utiliser la salle informatique pour son cours se retrouvait avec un certain nombre de postes de travails qui avaient un fonctionnement erratique.

La solution trouvée pour solutionner ce problème.

Un logiciel qui givre le disque dur.

Avant le début de l'année scolaire on installe sur les postes de travail tous les logiciels métiers que demandent les professeurs. (Ce qui est aussi fait pendant les autres vacances scolaires.)

On en profite pour mettre à jours tous les logiciels standards (et les anti-virus).

Puis un givre les postes.

Durant les cours les élèves peuvent modifier ce qu'ils veulent sur les postes.

Mais, à la fin du cours, il suffit d'éteindre les postes de travail, puis de les rallumer pour retrouver le poste avec son fonctionnement originel.

Les modifications apportées par les élèves ne sont pas retenues, seuls les fichiers enregistrés sur les serveurs sont gardés.

C'était une solution simple qui a répondu à une problématique identifiée.

Mais il fallait impérativement bloquer toutes les demandes de mise à jour sur tous les postes si non ces demandes auraient saturé l'accès internet.

Résumé

Il faut donc bien identifier le risque et trouver une solution qui limite le risque tout en étant la moins contraignante possible pour l'utilisateur.

Mais ne pas oublier que toutes les solutions ont une faille et, par exemple, pour le collège on avait oublié de verrouiller le BIOS par un mot de passe.

****
****

Mais vous pouvez faire ceci, chez vous, pour Surfer sur internet en toute sécurité. (et ceci gratuitement.)

Il suffit d'utiliser TAILS sur une clef USB.

Tails est une distribution Linux Unbouto complètement paramétrée et préinstallée avec un tas de logiciels libres de type Open-Office, Tor, etc.. (www.tails.net)

Suivez la procédure facile à suivre sur Internet pour installer Tail sur une Clef USB. (Clef de 8 Go ou plus)

Le plus compliqué est de booter sur la Clef USB. Pour cela il faut modifier le Bios de votre machine.

En suite vous utilisez TOR pour vous connecter à Internet et DuckDuckGo comme moteur de recherche.

Vous pouvez trouver tous les sites cachés d'internet y compris les sites en onion. (www.xxx.onion)

Quand vous arrêtez votre ordinateur rien n'a été conservé et donc aucune trace n'est laissée sur votre ordinateur.

Néanmoins deux choses à retenir.

Si vous donnez accès au disque dur de votre ordinateur, pour sauvegarder des fichiers copiés sur Internet, vous créer une faille de sécurité dans Tails.

Et d'autre part Tails ne vous protège pas du peer to peer de type Torrent. Puisque dans ce cas vous laissez les personnes venir sur votre ordinateur chercher les Torrents donc vous donnez l'adresse IP de votre Box Internet à vos utilisateurs Torrent. Pour utiliser des Torrents en toute sécurité il vous faut un VPN