CYBERSÉCURITÉ

NOUS SOMMES TOUS CONCERNÉS

PDF

Sur ordinateur, smartphone ou internet, adopte les bons réflexes !



IFSB

cases.lu
Cyberworld Awareness and Security Enhancement Services
LUXEMBOURG

CHAMBRE DES METIERS
Luxembourg

Cybersécurité n°5 : Mises à jour

CLEE USB PIEGEE

Tout comme une voiture dont on souhaite assurer la longévité, un ordinateur, un smartphone, ou une tablette doit être entretenu pour conserver un fonctionnement optimal.

Les mises à jour ; pourquoi ?

Dans chaque système d'exploitation (Android, IOS, MacOS, Windows,…), logiciel ou application, des vulnérabilités existent.
Les cyberattaquants exploitent ces vulnérabilités pour mener à bien leurs opérations.

Bien souvent, ces failles de sécurités sont découvertes et corrigées par les éditeurs. Ces derniers, proposent alors aux utilisateurs des mises à jour de sécurité.

Malheureusement un bon nombre d'utilisateurs ne procèdent pas à ces mises à jour rapidement. Par conséquent, ils restent vulnérables encore longtemps après la découverte et la correction des failles.

Mettre à jour ses logiciels dès que cela est possible, permet de bénéficier en permanence de la meilleure protection.

Comment se protéger :

- Configurez vos logiciels pour que les mises à jour de sécurité s'installent automatiquement.
- Téléchargez les correctifs de sécurité disponibles.
- Utilisez exclusivement les sites officiels des éditeurs.

PEN USB PERDIDA

Tal como um automóvel a que queremos assegurar a longevidade, um computador, smartphone ou tablet deve ser mantido de forma a assegurar o seu bom funcionamento.

Pen USB perdida ou ciberataque?! essa é a dúvida

Existem vulnerabilidades em cada sistema operativo (Android, IOS, MacOS, Windows, etc.), software ou aplicação.
Os atacantes cibernéticos exploram essas vulnerabilidades para realizar as suas operações.

Frequentemente, essas falhas de segurança são descobertas e corrigidas pelos editores. Estes últimos, propõem aos utilizadores atualizações de segurança.

Infelizmente, muitos utilizadores não realizam estas atualizações rapidamente. Por esse motivo, permanecem vulneráveis depois das falhas serem descobertas e corrigidas.

Atualizar o seu software o mais rapidamente possível permite beneficiar permanentemente da melhor proteção.

Como se proteger:

- Configure o seu software para instalar as atualizações de segurança automaticamente.
- Descarregue as atualizações de correção de segurança disponíveis.
- Use exclusivamente os sites oficiais dos editores.

Cybersécurité n°5 : Mises à jour

AKTUALISIERUNGEN

Genau wie ein Auto, das möglichst lange fahrtüchtig sein soll, müssen auch Computer, Smartphones oder Tablets gewartet werden, damit ihre optimale Funktionsfähigkeit gewährleistet bleibt.

Wozu Aktualisierungen?

Betriebssysteme – ob Android, IOS, MacOS, Windows usw. –, Software oder Anwendungen haben allesamt Schwachstellen.
Hacker nutzen diese Schwachstellen aus, um erfolgreiche Angriffe durchzuführen.

Diese Sicherheitslücken werden jedoch häufig von Softwareherstellern entdeckt und behoben. Letztere stellen den Benutzern dann Sicherheits-Updates zur Verfügung.

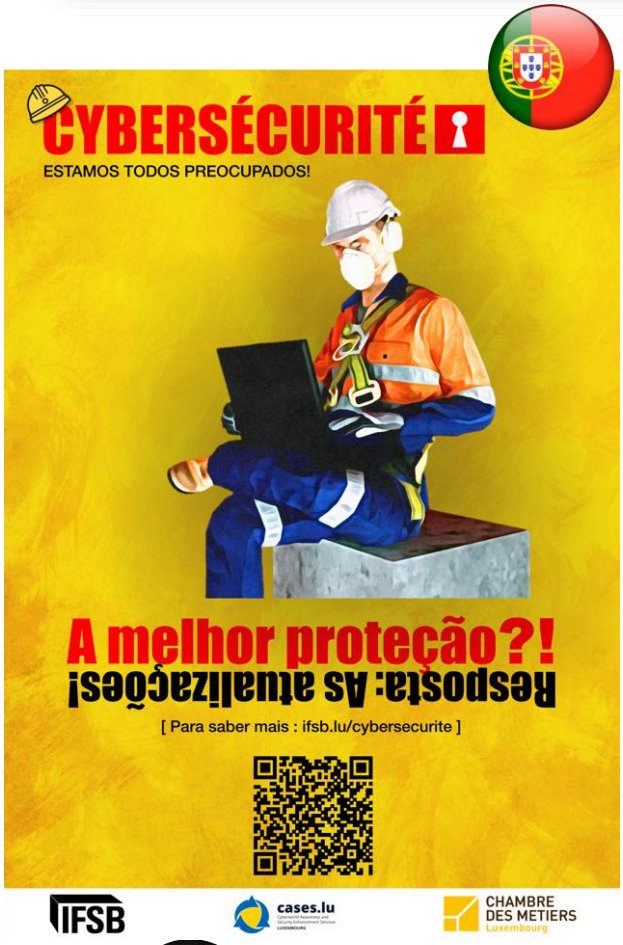
Bedauerlicherweise unterlassen es sehr viele Benutzer, diese Updates umgehend aufzuspielen. Folglich bleiben sie noch lange Zeit nach Entdeckung und Behebung der Schwachstellen anfällig.

Wer seine Software regelmäßig aktualisiert, sobald dies möglich ist, ist dauerhaft optimal geschützt.

So schützen Sie sich:

- Stellen Sie Ihre Software so ein, dass Sicherheits-Updates automatisch installiert werden.
- Laden Sie die verfügbaren Sicherheitspatches herunter.
- Laden Sie Patches nur von den offiziellen Websites der Hersteller herunter.

Cybersécurité n°5 : Mises à jour



IFSB

cases.lu
Cyberworld Awareness and Security Enhancement Services
LUXEMBOURG

CHAMBRE DES METIERS Luxembourg