



Rencontre avec Magda Chelly : cybersécurité à Singapour

Les cyberattaques en Asie Pacifique ont triplé entre janvier et mars 2020. Pour ne pas devenir une proie, Singapour Live a rencontré **Magda Chelly**, fondatrice de *Responsible Cyber* et spécialiste de la cybersécurité.

Magda Chelly : une entrepreneuse hors du commun

Singapour Live est fan de **Magda Chelly** et son **hilarant Sunday Cyber Show** façon John Oliver. Découvrons cette **personnalité de serial entrepreneuse hors du commun** qui parle anglais, français, arabe, polonais, italien et un peu de russe et d'espagnol. On est bluffé



Responsible Cyber fondé par Magda Chelly

Magda arrive à Singapour en 2015, après quelques mois de missions humanitaires en Asie. Elle y trouve du travail dans une société française de services informatiques puis décide de fonder sa propre entreprise dans le domaine de la formation, du conseil et de la **cybersécurité**.

Ses modèles sont les créateurs de start-up qui ont réussi à créer de la valeur et à revendre leurs entreprises à de grands groupes. Elle aime aussi côtoyer des gens de tous âges, de différents milieux sociaux, expériences, formations pour trouver son inspiration. Ses motivations sont la création, l'apport de valeur, l'autonomie et sa propre progression en tant que personne et en tant que professionnelle.

C'est pendant ses études à **Telecom Paris** qu'elle a commencé à tester les vulnérabilités de certains systèmes, par jeu et par curiosité. Son **doctorat en télécommunications** en poche, elle travaille au service informatique d'une grosse société d'assurance française puis pour une société de conseil et services informatiques.

Elle crée une première société de formation à domicile puis décide de quitter la France pour rejoindre un grand opérateur de télécommunications au Qatar.



Magda et une partie de son équipe: Tom Philippe, Daniel Lim, Jia Zheng Wen, Mikko Laaksonen

L'aventure Responsible Cyber

Aujourd'hui, elle est à la tête de **Responsible Cyber**, une entreprise de 7 employés, dont 2 français. Elle est très occupée, avec en cours : une levée de fonds et le développement d'une plate-forme d'identification et d'évaluation des cyber risques. **Ses clients sont principalement des grands groupes** européens ou américains qui recherchent des personnes capables de **bâtir des stratégies et des tactiques de protection vis-à-vis des risques cyber**.

Responsible Cyber propose du **conseil**, des cours de **sensibilisation à la cybersécurité**, une cartographie des **risques cyber**, la mise en oeuvre de **contrôles**, aussi des **tests d'intrusion** et de vulnérabilité. Elle a **en outre** une **offre dédiée aux petites entreprises**, mais ces dernières sont souvent réticentes à installer des systèmes de cybersécurité de manière proactive. C'est plutôt en réaction à une première attaque que ces entreprises vont mettre en oeuvre des systèmes de protection.



Responsable Cyber participe à ICE71, un programme pour aider les start-up à développer leur business à Singapour et dans la région Asie Pacifique.

Elle participe activement aux travaux de plusieurs associations pour **promouvoir les femmes dans les métiers de la sécurité** et elle est une **conférencière** recherchée, représentée par le London Speakers Bureau.



Magda lors d'une conférence en Malaisie.

Nous protéger des cyber attaques

Singapour Live a saisi l'opportunité de la rencontre pour glaner quelques conseils pour le télétravail que nous pratiquons tous à des degrés divers en ces temps de crise. En effet, **les cyberattaques en Asie Pacifique ont triplé entre janvier et mars 2020.**

Magda nous apprend que **les cybercriminels font eux aussi des business plans et exploitent toutes failles des systèmes.** Ils exploitent aussi les failles des personnes dont le comportement est si perturbé en temps de crise qu'elles deviennent des proies faciles. Les cybercriminels cherchent à mettre la main sur des données personnelles ou à s'introduire dans un réseau d'entreprise. Les employés sont en général mal préparés au télétravail. Et comme ils sont en **mode panique** ou survie : ils cliquent sur tout ce qui pourrait contenir une information ou une promesse rassurante.



Magda pendant une formation de cybersécurité pour jeunes filles avec Madame Sim Ann, Senior Minister of State at the Ministry of Culture, Community and Youth and Ministry of Communications and Information.

Sept conseils pour votre cybersécurité

1. **Ne cliquez pas sur tout** ce que vous recevez, lien, image etc. Assurez-vous que l'expéditeur et la source sont dignes de confiance, sinon n'ouvrez pas et détruisez ce qui vous a été envoyé.
2. Les **systèmes à double authentification** sont maintenant gratuits et diminuent énormément le cyber risque. Utilisez-les dès que possible. Votre banque le fait déjà et presque tous les services publics singapouriens aussi.
3. **Mettez à jour vos systèmes** anti-virus et **vos applications** sur votre ordinateur et votre smartphone. Les failles de sécurité des anciennes versions sont bien connues des cyber criminels et sont autant de portes ouvertes pour accéder à vos données.
4. **Redémarrez votre ordinateur tous les jours**, les mises à jour se feront automatiquement au démarrage.
5. Vous pouvez deviner assez facilement ce qu'elle pense de l'identifiant ADMIN et du mot de passe **PASSWORD** ? Oui ? Alors changez ! Et **changez souvent, surtout pour votre routeur wifi**.
6. **Ne laissez pas les membres de la famille utiliser votre ordinateur du bureau**. Non pas qu'ils soient mal intentionnés, mais vous ne savez pas à quoi et avec qui ils vont se connecter.
7. Rappelez vous que tout ce que vous faites sur votre ordinateur de bureau est enregistré et peut être retrouvé. **Il n'y a pas de notion de confidentialité ou de vie privée.**



Mikko Laaksonen, Magda et les journalistes de ITSP Magazine.

Magda recommande le **site du gouvernement GOSAFEONLINE** pour en savoir plus sur la **sécurité en ligne pour les particuliers**. Personne ne peut travailler aujourd'hui sans la technologie, il faut donc apprendre à déployer des solutions qui correspondent aux risques encourus.

Alors prenez soin de vous et de vos données !

Marie-Hélène Mansard