SENSIBILISATION

Aux dangers d'internet

Pour les adultes..

Les arnaques les plus fréquentes :

- Les faux sites internet
- Les fake news (fausses informations)
- Les courriels d'hameçonnage
- Les arnaques aux cadeaux
- Les arnaques aux supports techniques
- Les malveillants (virus, cheval de Troie, malware, adware..)
- ...

MARCOSERVICES – INFORMATIQUE LANGON

Depuis 2011 implanté sur le secteur de Langon. Prestataire en réparation informatique et en initiation informatique. Depuis 2017 nous sommes référent en CyberCriminalité informatique.


pirate informatique
cyberattaque
programme
informatique
virus
hacker
logiciel espion
spam
cybercriminalité
email
menace
attaque
internet
sécurité
réseau
code
intrusion
piratage
ordinateur
programmation

Agir contre les Ransomwares

Agir contre les Ransomwares et faux support technique

MarcoServices – Informatique Langon, est un professionnel référencé auprès de la https://www.cybermalveillance.gouv.fr. Mon rôle faire remonter les informations des faux support technique, des courriels que vous recevez et dont vous êtes infecté. Lors des interventions je collecte les informations et votre identité reste anonyme. Le but est de faire remonter le plus d'informations pour lancer des procédures de justice.

2011

MarcoServices – informatique Langon

2012

Partenaire avec le n°1 KASPERSKY LAB

2017

Partenaire Cybermalveillance.gouv.fr

2019

Attestation de suivi en CyberSécurité auprès de l'ANSSI
(Agence Nationale de la Sécurité des Système Informatique)

2020-2021

Formations en CyberSécurité

2022

Partenariat avec ESET antivirus

SecNum académie
ANSSI

ATTESTATION DE SUIVI

« Je soussigné, **M. Pascal Chour**, responsable du centre de formation de l'Agence nationale de sécurité des systèmes d'information (ANSSI), atteste que **M. MARC** [redacted] a suivi avec succès les cours des quatre modules du MOOC SecNum*académie* et obtenu les scores suivants aux évaluations :

MODULES	DATE DE L'ÉVALUATION	SCORE
PANORAMA DE LA SSI	04/11/2019	94%
SÉCURITÉ DE L'AUTHENTIFICATION	06/11/2019	80%
SÉCURITÉ SUR INTERNET	07/11/2019	96%
SÉCURITÉ DU POSTE DE TRAVAIL ET NOMADISME	07/11/2019	94%

www.secnumacademie.gouv.fr

Fait le 19 Mars 2020
Pascal Chour

Pensez-vous être anonyme sur internet ?

Non, vous n'êtes pas anonyme derrière votre écran d'ordinateur, de Téléphone ou de tablette. Chaque connexion internet a une signature numérique. Cette signature c'est comme la plaque d'immatriculation de votre voiture. Elle ne change pas. Nous partons du principe que vous êtes responsable de vos agissements sur l'ordinateur. On appelle cela une adresse IP (pour connaitre là votre, vous devez vous connecter sur le site www.mon-ip.com).

Qu'est ce qu'un Ransomware ?

Il faut d’abord commencer par le début. Un ransomware est un logiciel malveillant qui utilise plusieurs méthodes pour infecter les dispositifs, encodage de quelques ou tous les fichiers de l’appareil et vous demande de payer une rançon pour récupérer l’accès à vos précieuses données.

Le logiciel peut infecter votre ordinateur si, par exemple, vous connectez une clé USB inconnue à votre ordinateur, visitez un site malveillant, ou téléchargez et exécutez un fichier malveillant que vous avez téléchargé sur Internet ou reçu en pièce jointe.

Vous pouvez même être touché par un ransomware si vous ne faites rien de mal mais que votre ordinateur est sur le même réseau que celui d’un dispositif infecté.

Il existe même un ransomware qui ressemble à une mise à jour de Microsoft Windows.

Les nouvelles demandent de piège à la WEBCAM est un paiement en bitcoin (ou en toute autre crypto-monnaie) et c’est pourquoi il est très difficile à surveiller et de remonter jusqu'au commanditaire.

Devrais-je payer la rançon ?

NON !

Comment éviter les risques…

1- Disposez d'une bonne protection en utilisant KASPERSKY ou ESET

2- Suivre une formation de sensibilisation des dangers d'internet

3- Vous devez…

4- Vous croyez que nous allons tout vous dire dans cet extrait

5- Offrez une formation de sensibilisation des dangers d'internet à vos :
Parents, grand-parents

6- Oubliez pas la sensibilisation pour les ados contre le cyberharcèlement et les applications

Qu'est ce qu'un faux support technique, soit un Ransomware

Un faux support technique, c'est quand on dit, que votre ordinateur va infecter tout le reseau internet.
C'est quand on dit d'appeler un numéro de téléphone pour vous débloquer.

Un ransomware ou rançongiciel en français est une forme de malware qui subtilise des données de l'utilisateur à son insu. L'attaquant chiffre (crypte) les données de la victime et demande une rançon en échange de la clé privée. Un ransomware est distribué entre autres via des pièces jointes, des programmes infectés et des sites Web compromis. Les experts en sécurité font parfois référence à un programme malveillant de ransomware en tant que cryptovirus, crypto-trojan ou crypto-tour.

Le ransomware verrouille votre ordinateur ou chiffre vos données et les libère uniquement après avoir payé une rançon.
Fondamentalement, les ordinateurs de bureau, les serveurs, les portables, les tablettes et les smartphones sont affectés quel que soit les systèmes d'exploitation courants utilisés tels que Windows, Mac OS X, Android, iOS et Linux.

pour en savoir d'avantage, suivez le cours..

La question : que dois-je faire alors ?

pour le savoir, suivez le cours..

Si j'appelle je risque quoi ?
Vous allez payer une rançon de déblocage qui peut aller jusqu'à 590€, cela commence de la façon suivante :

!! Inscrivez-vous pour le cours !!

FORMATION POUR ADULTES EN SENSIBILISATION AUX DANGERS SUR INTERNET

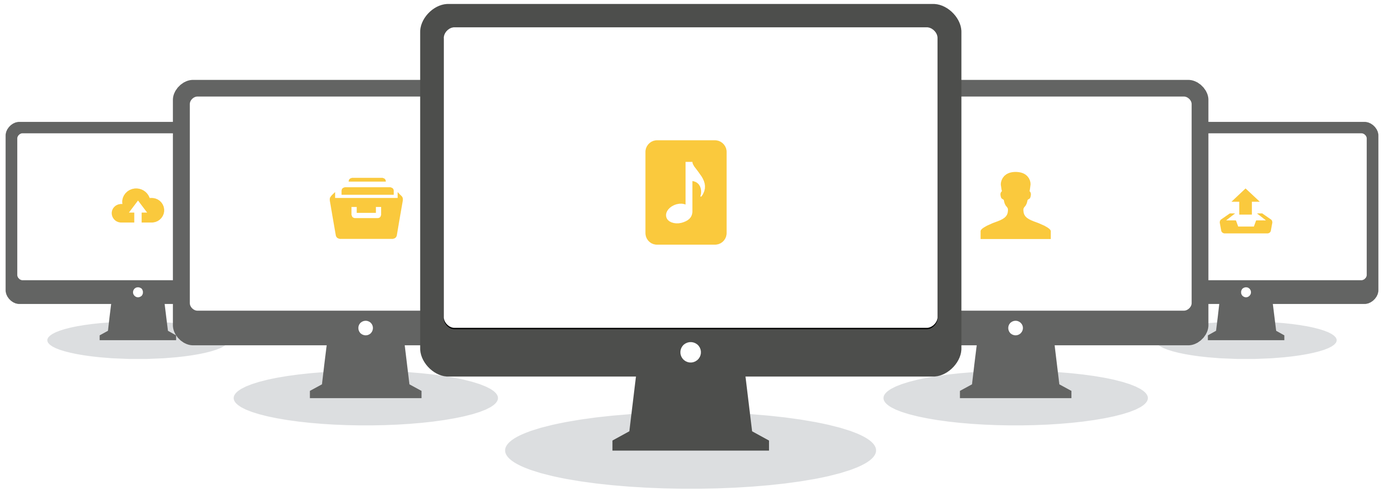
Sensibilisation

99€

abattement fiscal de 50% sur le tarif

Durée 1h30 de sensibilisation des dangers de l'internet pour adultes et seniors
+ Accès à un site dédié

Une bonne protection..



VOS FICHIERS SERONT EN SECURITE

Vos documents, vos photos de souvenirs, vos vidéos persos, vos données, n'ont pas de prix ! Une demande de raçon, il s'agit d'un cambriolage de votre intimité. La personne vous bloque votre ordinateur, mais il voit tout de vous.. Alors un bon geste pour vous protéger, une bonne protection sur votre informatique et vous pourrez éviter ce type de menaces et bien d'autres..

DITES VOUS CECI :

- Cela n'arrive pas qu'aux autres... Et que les autres c'est vous !

- Cela va être de plus en plus fréquent dans les années avenir

La cybercriminalité sur internet

Qui est le plus touchés :

- Les adultes et les seniors font souvent des erreurs d'inattention et/ou n'ont pas les bases..

→ Nous avons mis en place un tout nouveau programme de formation à la sensibilisation des dangers sur internet, spécialement pour les adultes. Pensez-y avant que le mal soit fait...

- Les adolescents entre 8 et 17 ans pour le cyberharcèlement

→ Nous avons également préparé un tout nouveau programme spécifique pour vos ados
Mais nous n'avons pas oubliez les parents dans cette formation de sensibilisation :)

C'est pourquoi faut pas avoir peur de faire intervenir un prestataire informatique référent en CyberMalveillance.

L'arnaque au faux support technique

« Extorquer de l'argent, à la victime en la poussant à laisser prendre le contrôle de sa machine pour faire semblant de la lui dépanner et lui installer des logiciels espions et faire souscrire des abonnements qui lui seront facturés le double du prix »

L'arnaque au faux support technique consiste à effrayer la victime par un message « votre ordinateur est infecté et va contaminer le réseau, vous devez appeler dans les 5min le numéro suivant sinon on bloque votre ordinateur » . Sachez que votre ordinateur ne peut pas infecter le réseau, sachez également que le numéro de téléphone appartient à la personne qui vient de vous infecter !
En aucun cas MICROSOFT vous demandera d'appeler, il s'agit d'une arnaque, ne cédez pas à la panique..

Si vous êtes victime :

- NE REPONDEZ PAS AUX SOLLICITATIONS et n'appelez jamais le numéro indiqué.
- VOUS PRENEZ UNE PHOTO DE VOTRE ECRAN AVEC VOTRE SMARTPHONE
- DEBRANCHEZ LE CABLE INTERNET OU LA BOX
- NE TOUCHEZ A RIEN
- NE JOUEZ PAS AU PRO DE L'INFORMATIQUE ou sur des forums avec des apprentis sorciers
- CONTACTEZ NOUS DIRECTEMENT AU 06.03.74.10.88 nous sommes reconnu comme prestataire référencé auprès de la CYBERMALVEILLANCE.GOUV.FR

→ **VOUS DEPOSEREZ UNE PLAINTE A LA BRIGADE DE GENDARMERIE DONT VOUS DEPENDEZ, APRES NOTRE INTERVENTION AVEC DES ELEMENTS QUE NOUS VOUS FOURNIRONS !**

DE NOTRE COTE, NOUS RELEVONS LES INFORMATIONS DES CYBERCRIMINELS POUR LES TRANSFERER A LA CYBERMALVEILLANCE.GOUV.FR

Les mesures préventives :

- *Appliquez de manière régulière et systématique les mises à jour de sécurité*
- Tenez à jour votre antivirus de confiance et lancez des analyses
- Évitez les sites non sûrs ou illicites
- N'ouvrez pas les courriels d'expéditeurs inconnu
- N'ouvrez pas les pièces jointes d'expéditeurs inconnu ou du style « mes photos, factures »
- Faites des sauvegardes régulières sur disque dur externe
- Ne laissez pas d'informations personnelles dans votre ordinateurs (documents, photos)

→ *VOUS AVEZ BESOIN D'UNE REMISE A NIVEAU OU APPRENDRE :*
- FAIRE DES SAUVEGARDES
- RENOMER DES FICHIERS
...

CONTACTEZ NOUS POUR UN COURS INFORMATIQUE

“ MarcoServices informatique Langon”

Pour un rendez-vous 6/7

Vous pouvez me joindre par téléphone pour un rendez-vous du lundi au samedi de 10h à 18h30.

Support par mail

Vous pouvez me contacter 7j/7 et vous aurez une réponse sous 24 à 48h. Pour plus de renseignements : informatique langon