Tiens ! Encore un spam pour utiliser mon compte CPF dans ma boîte mail ! Normalement ce message partirait directement dans la corbeille mais aujourd'hui je suis en congés alors j'ai un peu de temps devant moi et je me demande si je peux en savoir plus sur le "niveau" de cette arnaque.

Bon, ça commence mal pour l'arnaqueur car l'image d'en-tête ne s'affiche pas ! Et son adresse email n'est même pas camouflée. On sait donc directement que le message n'a pas été envoyé par Mon Compte Formation.

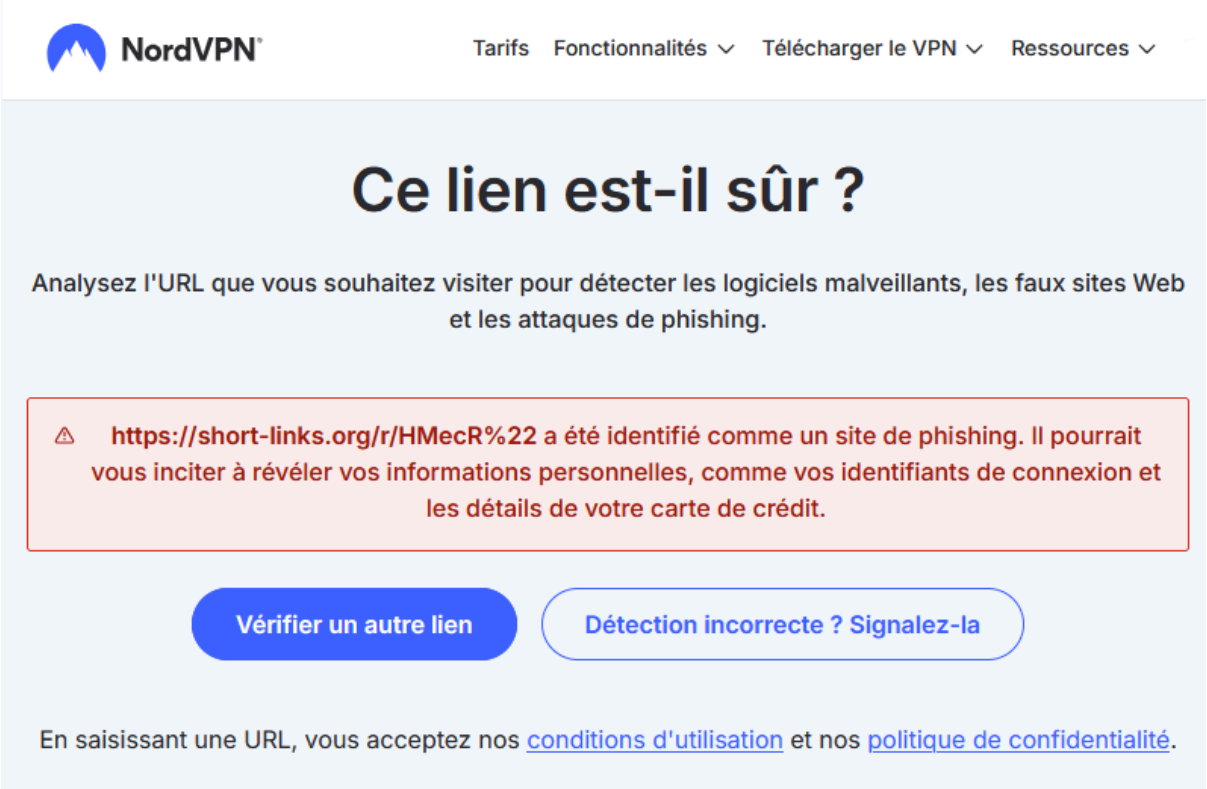
On pourrait s'arrêter là … mais

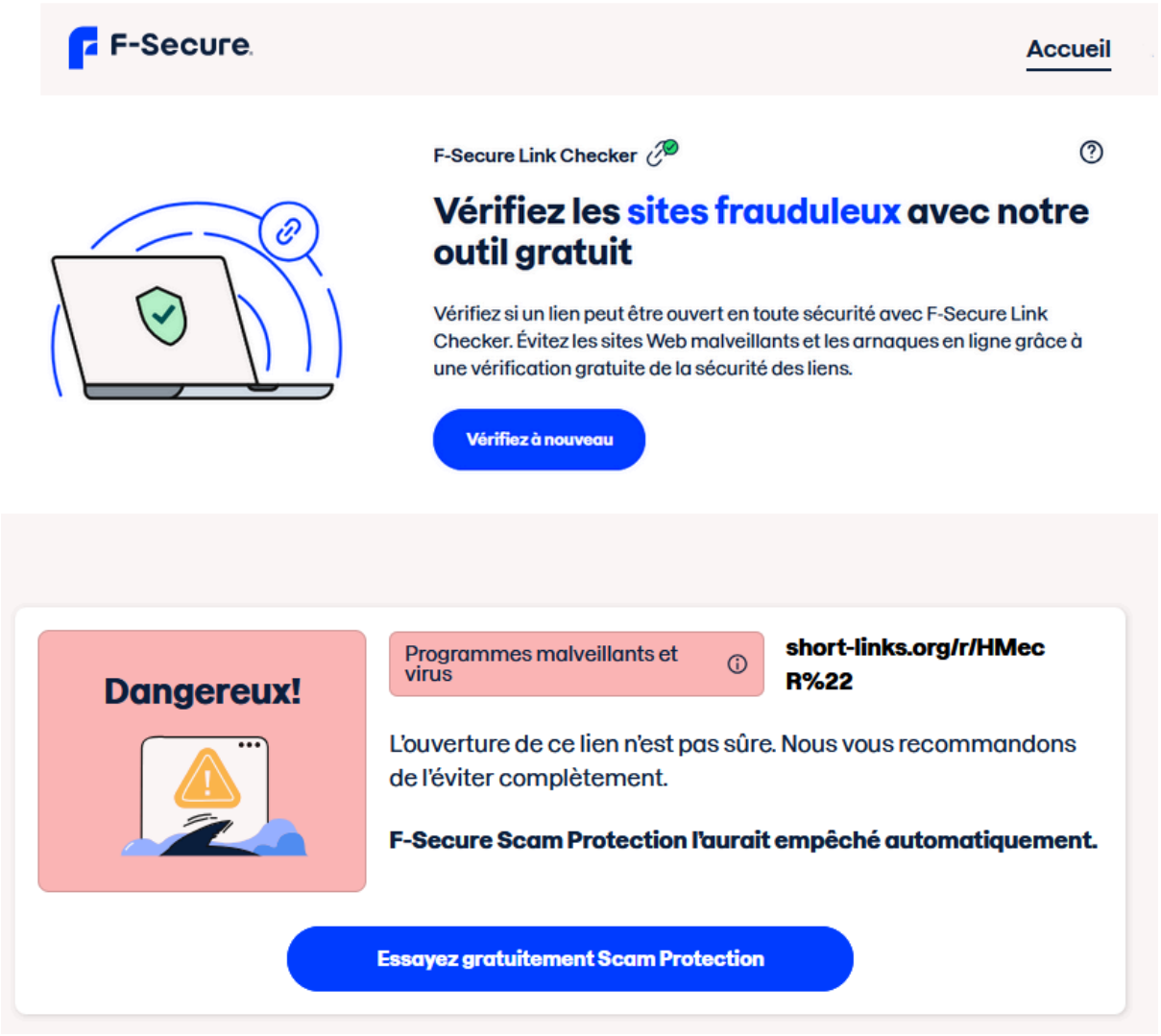
Ma curiosité est plus forte et comme j'ai encore un peu de temps devant moi je me dis que je vais tester ces outils de vérificateur de lien que certains logiciels de sécurité nous proposent.

Le lien vers le site de pishing se cache donc derrière le bouton "**Découvrez maintenant!**" et est un lien raccourci : https://short-links.org/r/HMecR

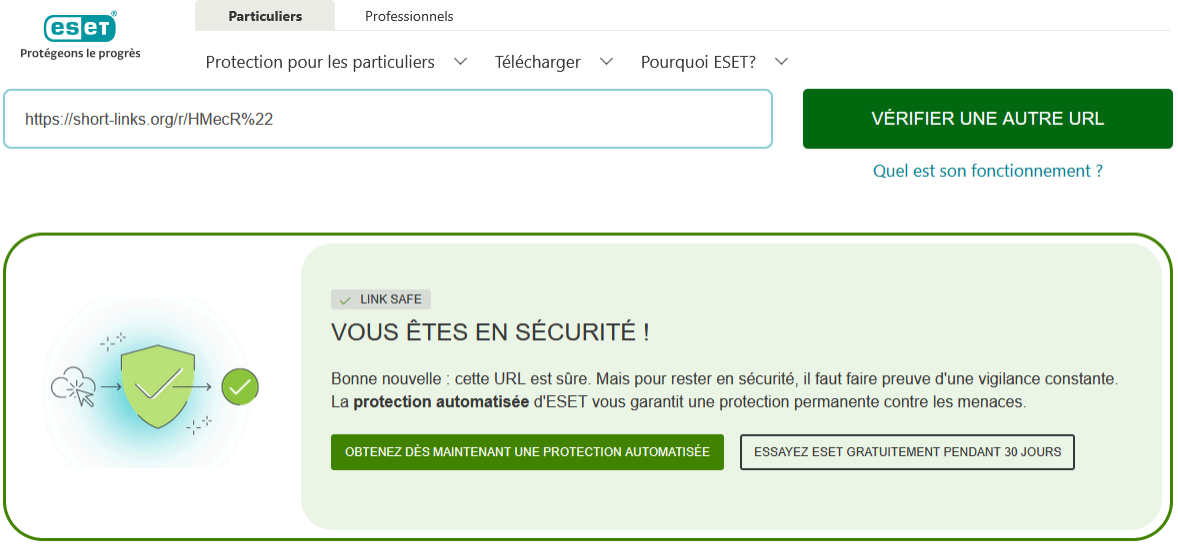
Testons donc ce lien suspect

Pour cela il existe des outils "sponsorisés" par des logiciels et c'est donc là que je commence :



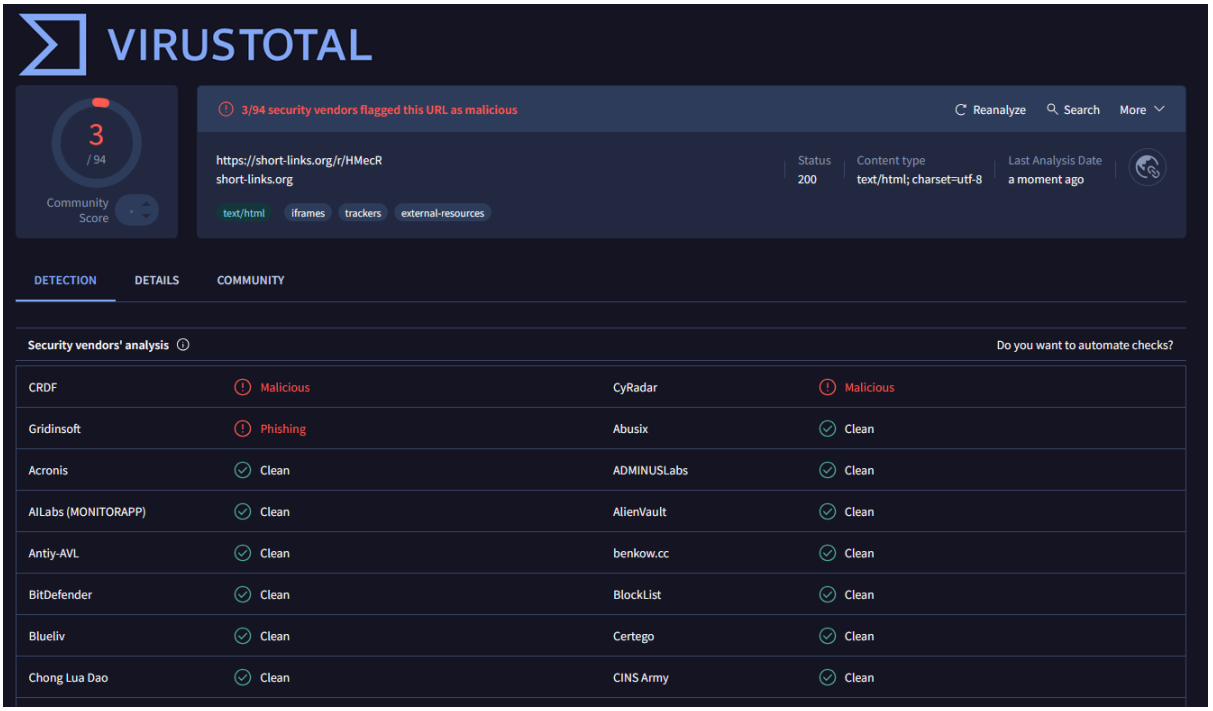


Si les 2 premiers vérificateurs me donnent une réponse positive à l'arnaque les 2 suivants me donneront un résultat différent :

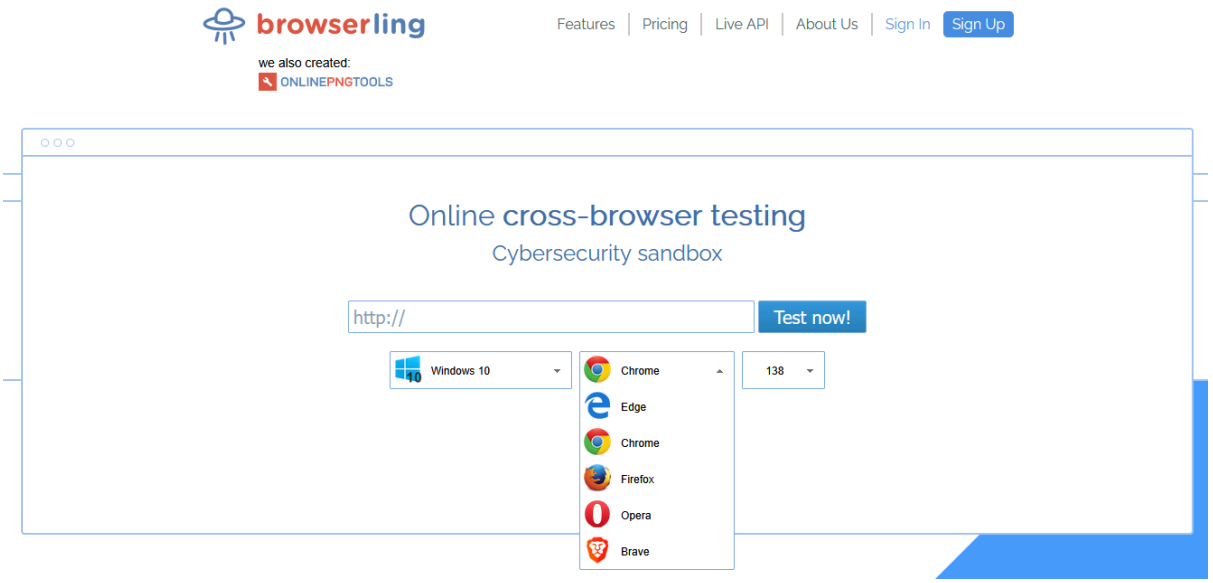


Deux partout la balle au centre !

Au vu de ces 2 réponses différentes on pourrait se demander qui a la bonne réponse … et donc le plus simple est peut-être de se diriger vers un site qui n'a pas de lien avec un opérateur qui tente de nous vendre une solution payante (ou gratuite mais avec des contreparties de collecte de vos données).

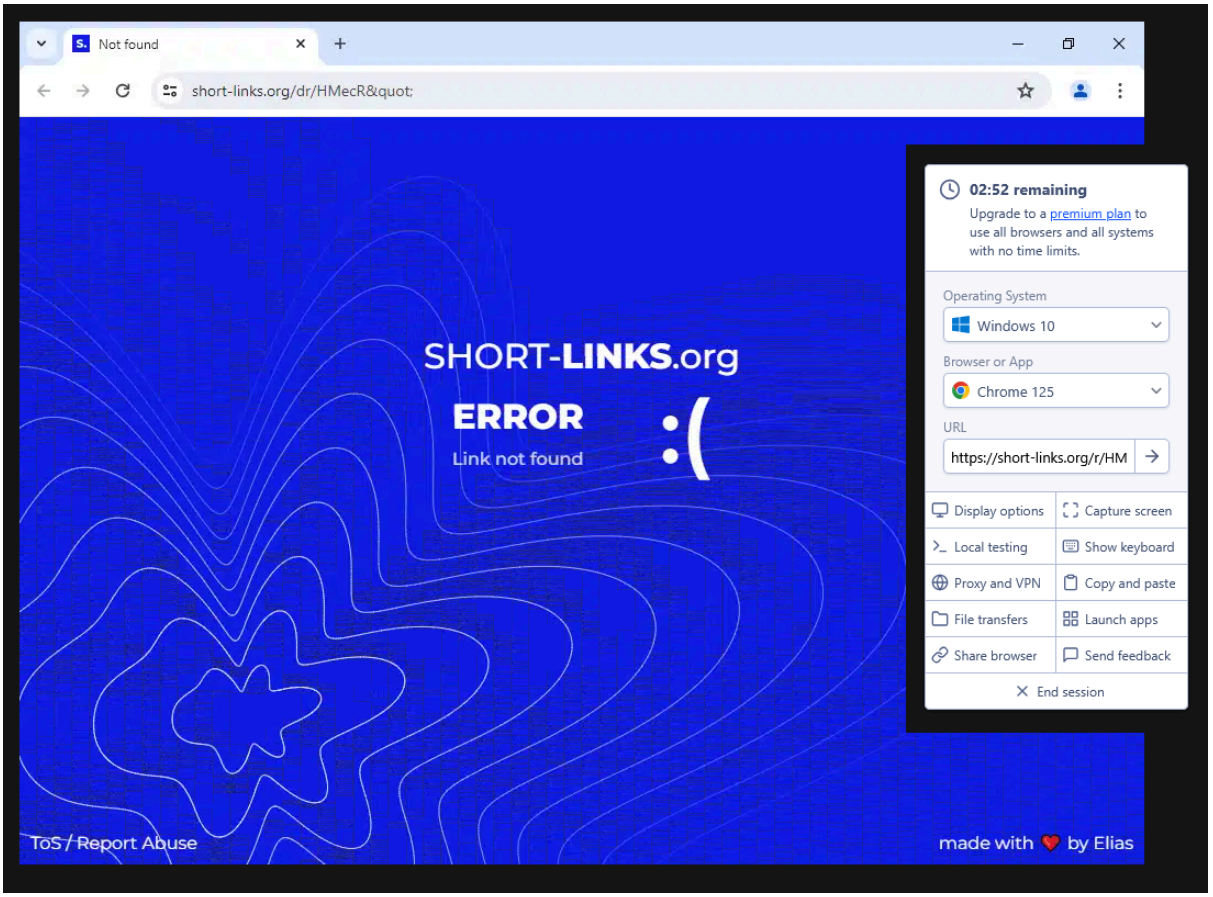


VirusTotal dispose de cet outil : https://www.virustotal.com/gui/home/url et l'analyse est là aussi à nuancer car la première réponse indique clairement un soucis, la seconde aussi en signalant même une tentative de phishing mais elle conclut en indiquant que c'est "clean" …



Browserling - https://www.browserling.com/ - dispose d'une solution intéressante pour les petits curieux qui veulent savoir ce qui se cache derrière ces liens sans subir les dangers de ce Phising.

Cet “émulateur” de navigateur va lancer une requête dans un faux navigateur et sur un système d'exploitation fictif (ici un navigateur Google Chrome sous Windows 10) et l’afficher au coeur du navigateur :



Nous avons alors enfin la réponse à notre curiosité ! Et sur ce coup ci on ne pourra pas voir à quoi ressemble le site d’arnaque car il a déjà été désactivé par hébergeur ou par le fournisseur de l’outil de redirection du lien court.

Mais maintenant vous avez les outils pour tester le prochain site d’arnaque que vous recevrez !