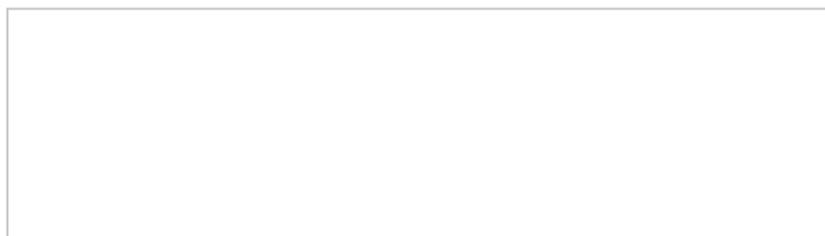


Tiens ! Encore un spam pour utiliser mon compte CPF dans ma boîte mail ! Normalement ce message partait directement dans la corbeille mais aujourd'hui je suis en congés alors j'ai un peu de temps devant moi et je me demande si je peux en savoir plus sur le "niveau" de cette arnaque.

Mise à jour de votre CPF.

Mon compte formation <noreply@fggjhbnm11.firebaseio.com>



MINISTÈRE DU TRAVAIL, DE L'EMPLOI ET DE L'INSERTION
COMPTE PERSONNEL DE FORMATION (CPF)

Bonjour,

Votre compte CPF vous permet d'accéder à des formations certifiantes 100 % prises en charge.

Choisissez votre formation et lancez-vous en quelques clics.

DÉCOUVREZ MAINTENANT!

Lien sécurisé • Authentification requise

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 phishing 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 :

The screenshot shows a web interface for NordVPN's security features. At the top, there is a navigation bar with the NordVPN logo, Tarifs, Fonctionnalités, Télécharger le VPN, and Ressources. The main heading is "Ce lien est-il sûr ?". Below it, a sub-instruction reads: "Analysez l'URL que vous souhaitez visiter pour détecter les logiciels malveillants, les faux sites Web et les attaques de phishing." A red warning box contains the text: "⚠️ <https://short-links.org/r/HMecR%22> a été identifié comme un site de phishing. Il pourrait vous inciter à révéler vos informations personnelles, comme vos identifiants de connexion et les détails de votre carte de crédit." At the bottom, there are two buttons: "Vérifier un autre lien" and "Détection incorrecte ? Signalez-la". A footer note states: "En saisissant une URL, vous acceptez nos [conditions d'utilisation](#) et nos [politique de confidentialité](#)".

F-Secure Link Checker 

Vérifiez les sites frauduleux avec notre outil gratuit

Vérifiez si un lien peut être ouvert en toute sécurité avec F-Secure Link Checker. Évitez les sites Web malveillants et les arnaques en ligne grâce à une vérification gratuite de la sécurité des liens.

[Vérifiez à nouveau](#)**Dangereux!**

Programmes malveillants et virus

short-links.org/r/HMec
R%22

L'ouverture de ce lien n'est pas sûre. Nous vous recommandons de l'éviter complètement.

F-Secure Scam Protection l'aurait empêché automatiquement.[Essayez gratuitement Scam Protection](#)

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



Particuliers

Professionnels

Protégeons le progrès

Protection pour les particuliers

Télécharger

Pourquoi ESET?

<https://short-links.org/r/HMecR%22>[VÉRIFIER UNE AUTRE URL](#)[Quel est son fonctionnement ?](#)**✓ LINK SAFE****VOUS ÊTES EN SÉCURITÉ !**

Bonne nouvelle : cette URL est sûre. Mais pour rester en sécurité, il faut faire preuve d'une vigilance constante. La **protection automatisée** d'ESET vous garantit une protection permanente contre les menaces.

[OBTENEZ DÈS MAINTENANT UNE PROTECTION AUTOMATISÉE](#)[ESSAYEZ ESET GRATUITEMENT PENDANT 30 JOURS](#)



Pour particuliers

Pour les petites entreprises

Pour Entreprises

Abonnements tout-en-un ▾ Sécurité des appareils ▾ Confidentialité



<https://short-links.org/r/HMecR%22>



Jusqu'ici, tout va bien



Ce lien ne présente aucun signe d'activité suspecte. Ne prenez pas le risque de faire des suppositions – notre dispositif de sécurité de premier ordre vérifie automatiquement la sécurité des liens et des sites Web. Essayez-le gratuitement pendant 30 jours !



[Essayer gratuitement](#)



[Vérifiez un autre lien](#)

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).

The screenshot shows the VirusTotal interface for the URL <https://short-links.org/r/HMeCR>. The top navigation bar includes 'Reanalyze', 'Search', and 'More'. Below the URL, it shows a status of 200, content type as text/html; charset=utf-8, and last analysis date as 'a moment ago'. The main content area is titled 'DETECTION' and lists various security vendors' analysis results:

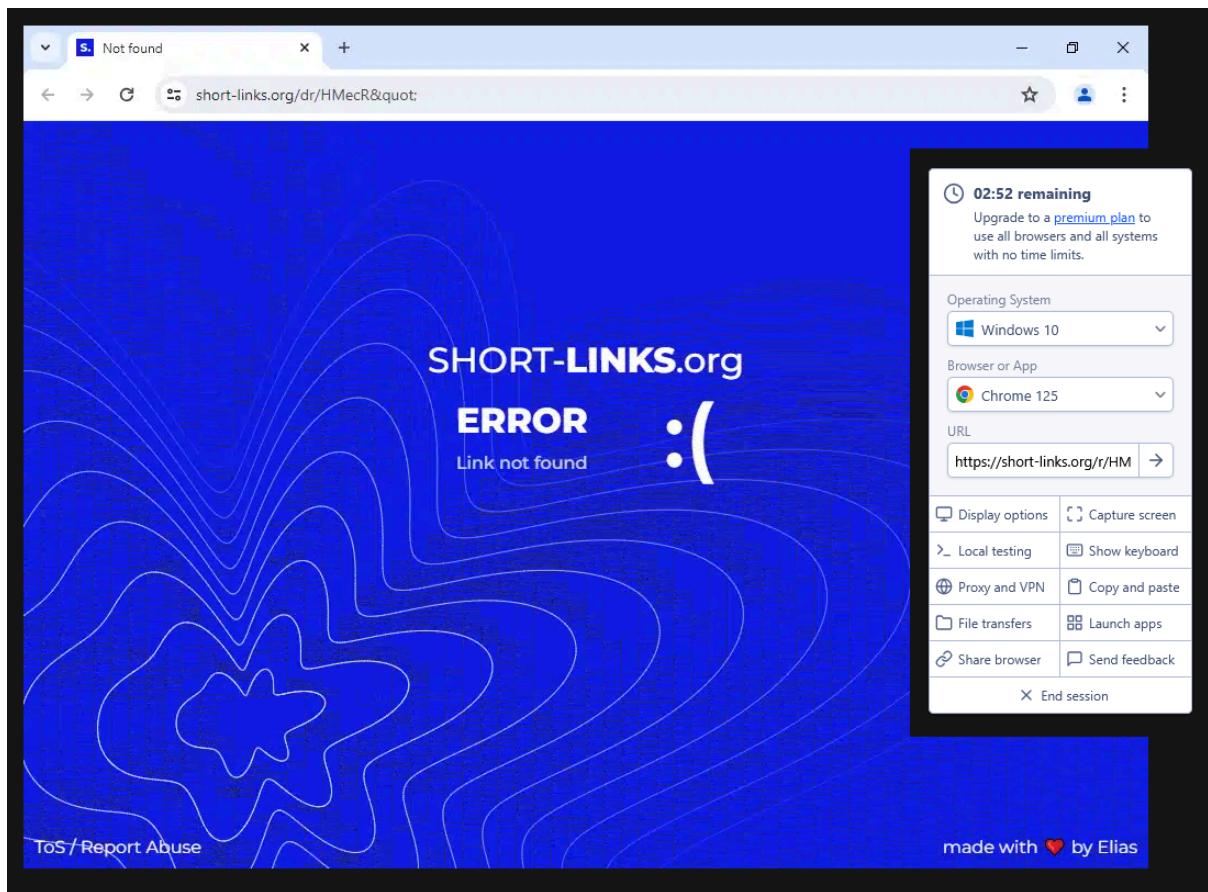
Vendor	Result	Vendor	Result
CRDF	Malicious	CyRadar	Malicious
Gridinsoft	Phishing	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean
AI Labs (MONITORAPP)	Clean	AlienVault	Clean
Antiy-AVL	Clean	benkow.cc	Clean
BitDefender	Clean	BlockList	Clean
Blueliv	Clean	Certego	Clean
Chong Lua Dao	Clean	CINS Army	Clean

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" ...

The screenshot shows the Browserling website, which offers an online cross-browser testing service. The main heading is 'Online cross-browser testing' and 'Cybersecurity sandbox'. A dropdown menu allows users to select a browser environment, currently set to 'Windows 10'. To the right of the dropdown is a list of supported browsers: Chrome, Edge, Firefox, Opera, and Brave. At the bottom right, there is a blue button labeled 'Test now!'

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 !