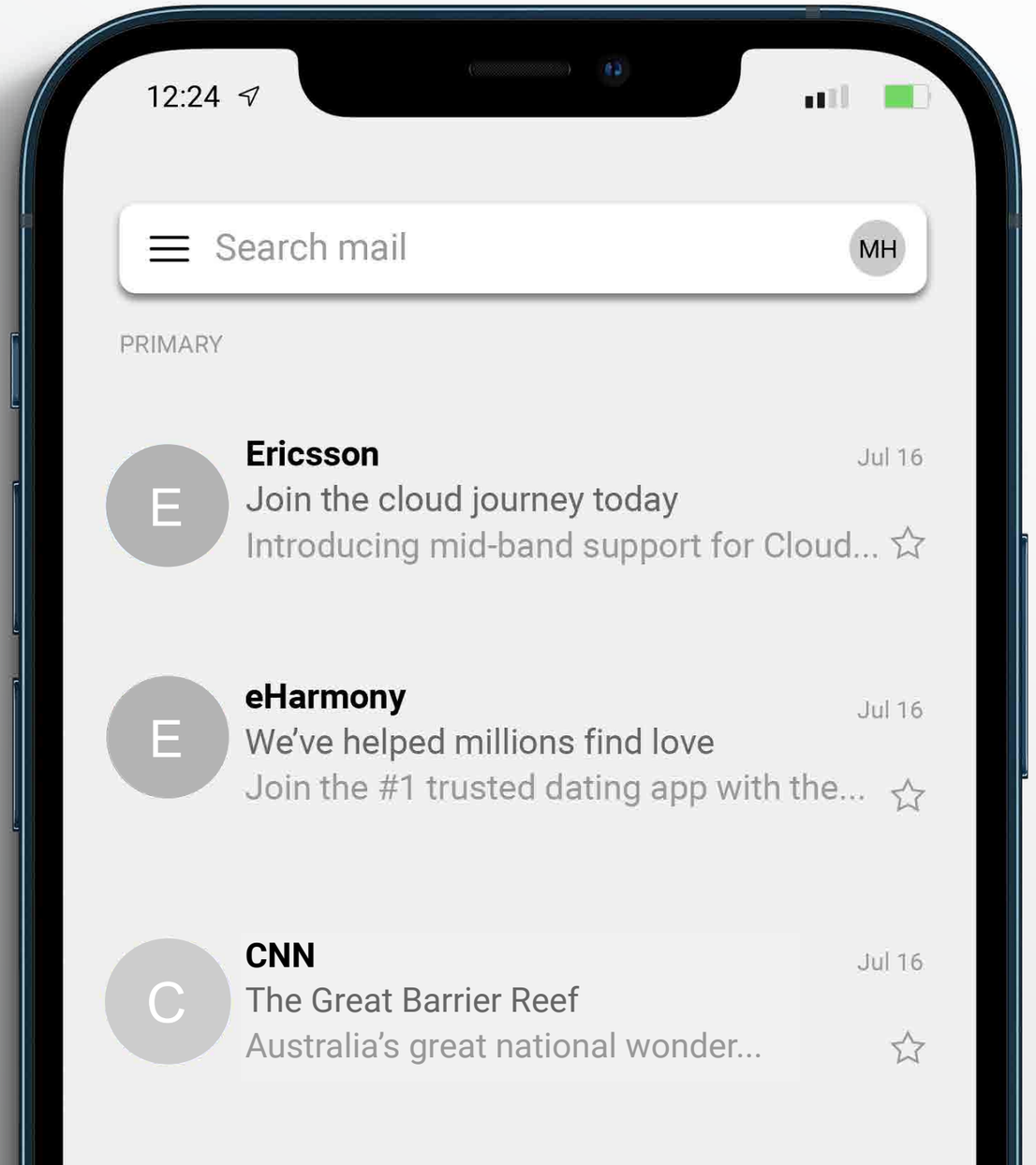
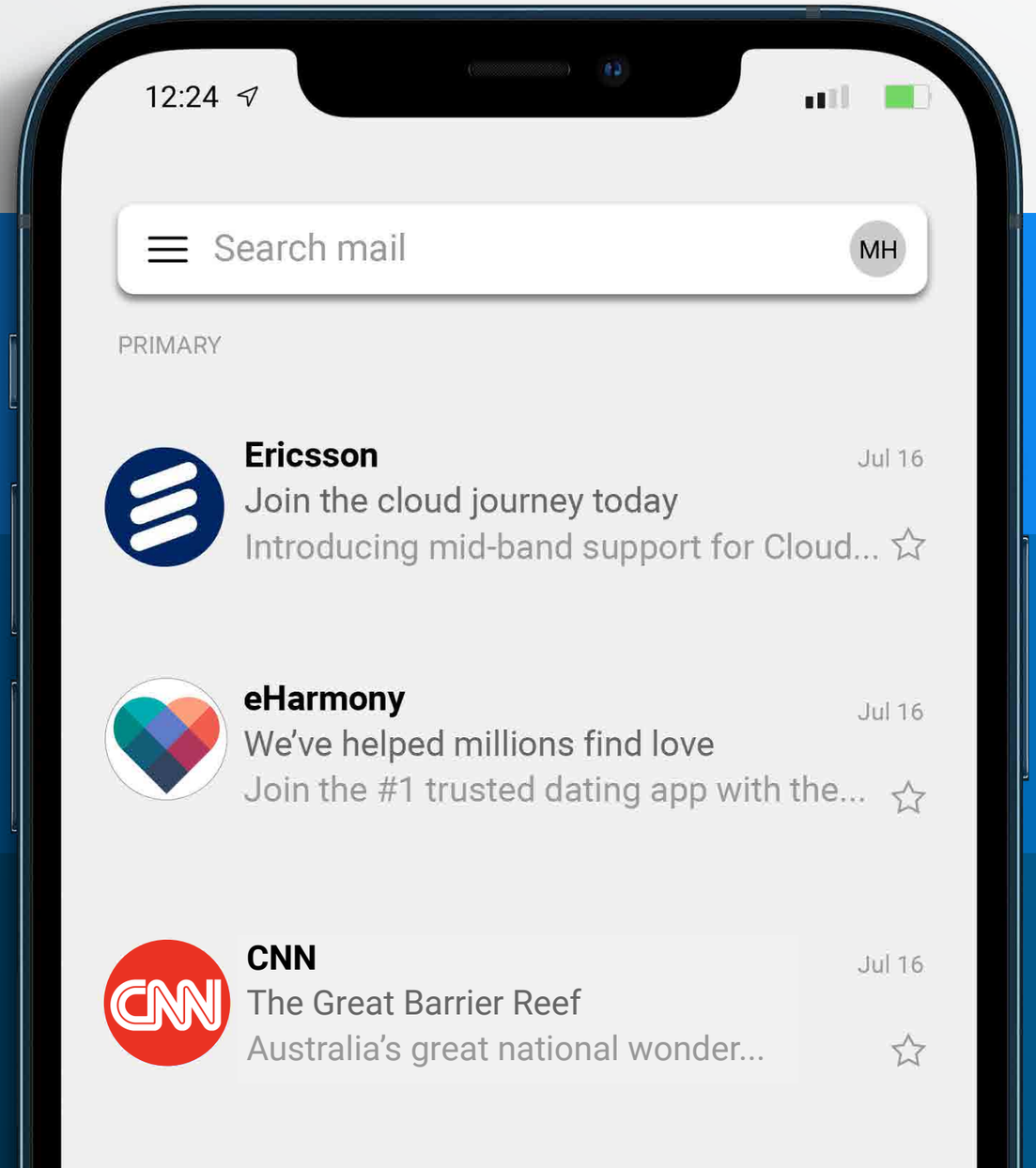
ON VÉRIFIE TOUT. ALORS POURQUOI L'E-MAIL DEVRAIT-IL FAIRE EXCEPTION ?

Coche bleue sur Twitter ou Tiktok, confirmation d'identité d'un appelant, affichage d'un sceau Smart Seal sur la page de paiement d'un site d'e-commerce… les preuves d'authenticité d'un utilisateur ou d'une marque sont de plus en plus courants sur la plupart des supports de communication. Cette vérification systématique des comptes publics rassure immédiatement sur le fait que la personne ou l'entreprise à l'origine du message est bien qui elle prétend être. Cette garantie d'authenticité renforce le lien de confiance, ce qui incite les marques à se soumettre à ce processus de vérification et à ainsi se démarquer de la concurrence.

LE PARADOXE DE L'E-MAIL

Le problème du plus ancien, du plus efficace et du plus utilisé des supports de communication numériques, c'est qu'il permet un complet anonymat, dans le sens où l'identité de chaque personne et de chaque marque, grande ou petite, s'est traditionnellement résumée à quelques lettres.





DU MOINS, JUSQU'À AUJOURD'HUI.

E-MAIL MARKETING : L'HEURE EST VENUE D'APPOSER VOTRE MARQUE

Développés dans le cadre d'une initiative révolutionnaire lancée en collaboration avec le BIMI (Brand Indicators for Message Identification) et divers éditeurs de clients de messagerie, les certificats VMC (Verified Mark Certificates) réalisent une grande première en vous permettant d'afficher votre logo dans la boîte de réception de vos clients, ce avant même qu'ils ne cliquent sur votre message. Dernière étape d'une procédure draconienne de sécurité et d'authentification des identités, les certificats VMC contribuent à renforcer la confiance dans la messagerie électronique.

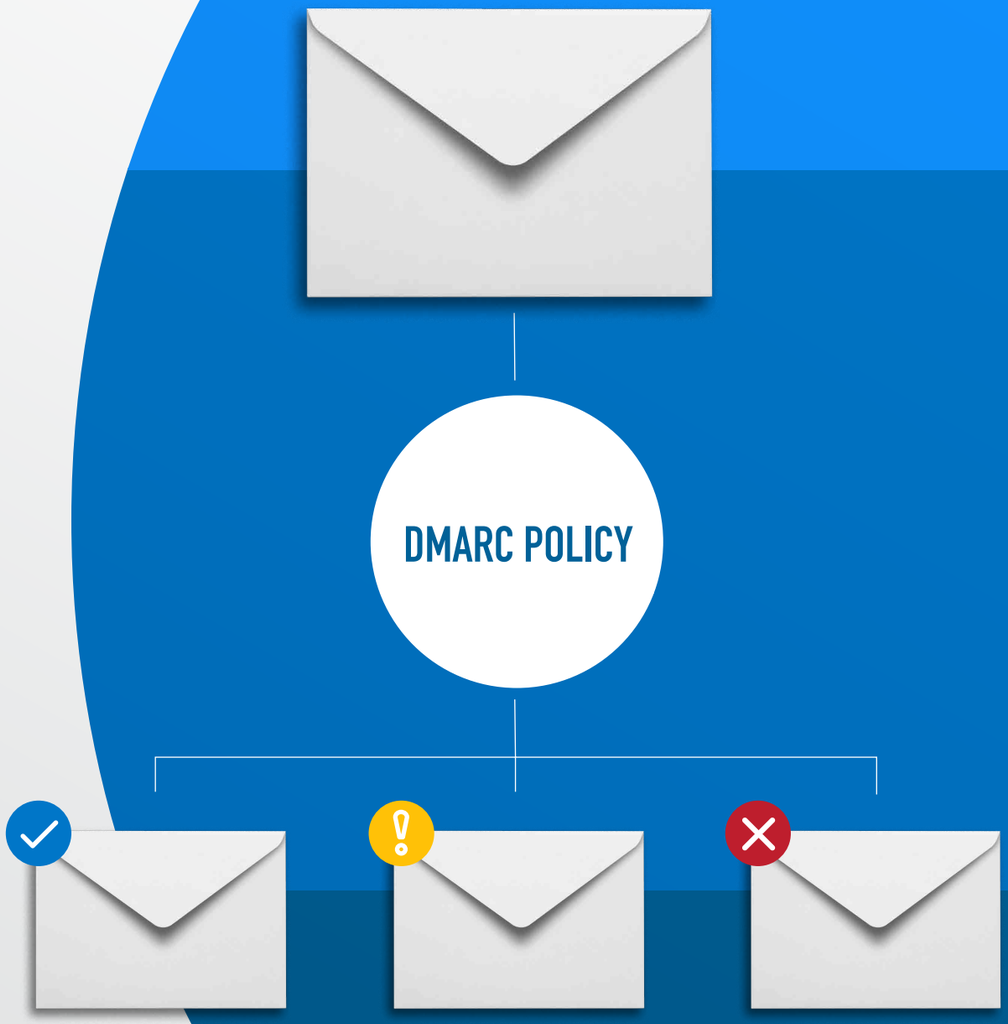
MARKETING ET IT : LA RÉCONCILIATION

Et puis il y a le volet sécurité. L'objectif principal du BIMI est d'inciter les marques à se conformer au protocole DMARC, tirant ainsi toute l'industrie vers le haut en rendant les communications plus difficiles à détourner. Ceci dit, malgré tous les efforts des équipes informatiques, l'application du protocole DMARC reste encore relativement faible à travers le monde. Du fait de sa longueur, ce processus est souvent reporté à plus tard, au profit d'initiatives plus urgentes à court terme . Le projet pilote BIMI/VMC vise à changer la donne en offrant aux entreprises un avantage concret et immédiat.

QU'EST-CE QUE LE DMARC ?

Abréviation de "Domain-based Message Authentication, Reporting and Conformance", le DMARC est un protocole de reporting et de politique d'authentification des e-mails. Basé sur les très répandus protocoles SPF et DKIM, le DMARC ajoute un lien vers le nom de domaine de l'expéditeur ("De:"), des politiques publiées pour le traitement des échecs d'authentification par le destinataire, et un reporting "destinataires à expéditeurs", le tout pour renforcer la protection du domaine contre les e-mails frauduleux.

Autrement dit, le DMARC offre aux professionnels de la sécurité davantage de transparence et de contrôle pour identifier avec précision, puis bloquer ou isoler plus rapidement les e-mails frauduleux. Fruit d'une mûre réflexion autour de quelques règles de bon sens, il permet aujourd'hui de protéger à la fois les consommateurs et les marques.



DES ATTAQUES PAR INGÉNIERIE SOCIALE SONT TRANSMISES PAR E-MAIL.

(source : https://enterprise.verizon.com/en-gb/resources/reports/dbir/)

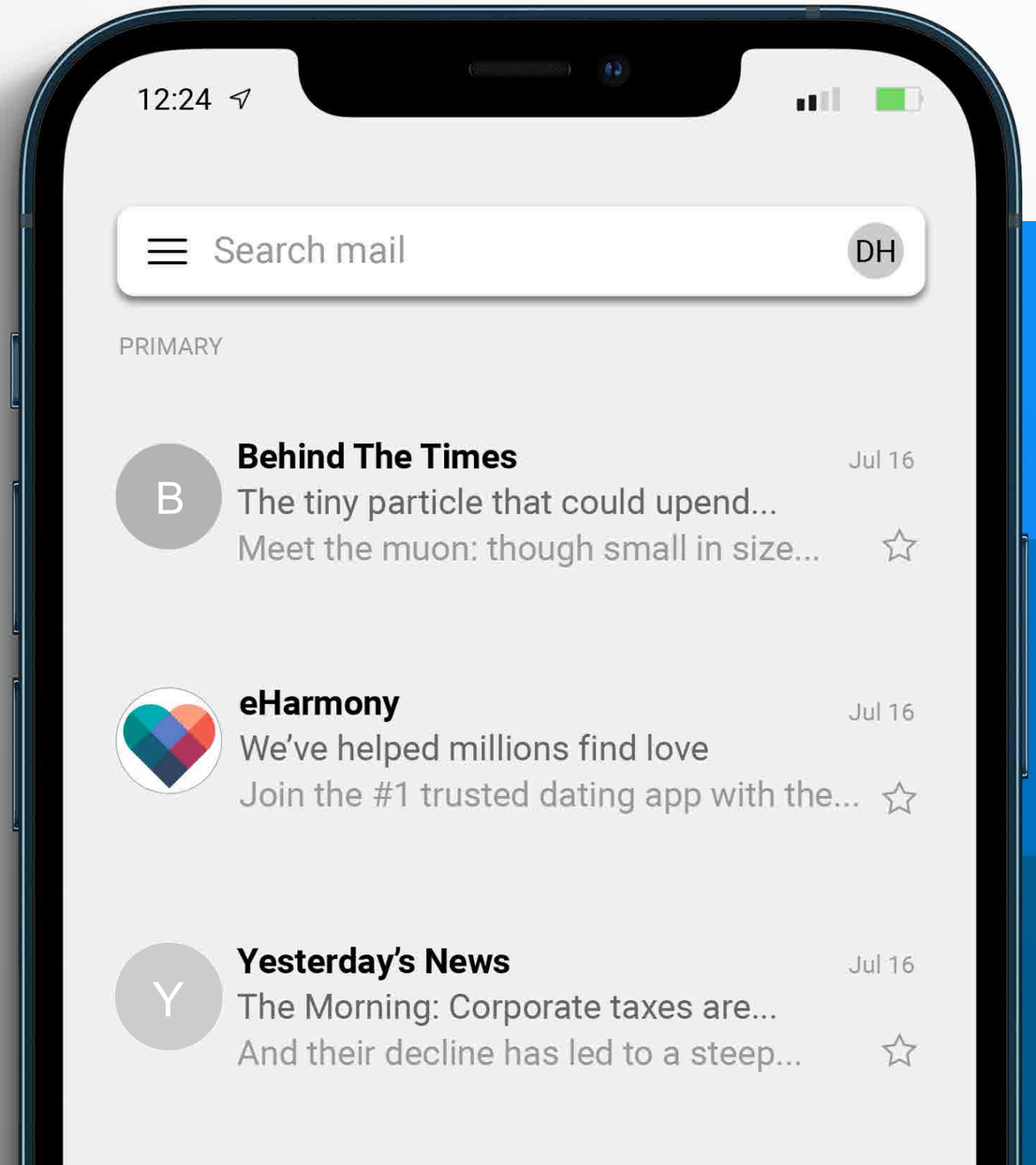
MARQUEZ DES POINTS

Un logo protégé par un certificat VMC ne s'affiche que lorsque le client de messagerie vérifie que l'enregistrement BIMI de votre entreprise indique bien une conformité au protocole DMARC. Cette vérification confirme que vous disposez des outils et avez mis en place les pratiques nécessaires pour prévenir les attaques de phishing et par usurpation d'identité (« spoofing »). L'Autorité de certification émettrice, en l'occurrence DigiCert, vérifiera également le logo de votre entreprise auprès de l'INPI, ou de tout autre office national des marques, pour s'assurer que vous êtes une entité légitime et reconnue, et validera l'acheteur du certificat VMC via un notaire mobile. Tout ceci permet de valider le droit de votre entreprise à afficher votre logo vérifié.

DigiCert + BIMI + VMC = E-mail vérifié

C'EST MAINTENANT QU'IL FAUT VOUS DÉMARQUER

De par leur nouveauté, les certificats VMC donnent aux primo-adoptants l'occasion de se différencier visuellement de leurs concurrents. Pour prendre un bon départ, suivez le guide.



01 APPLIQUEZ LE DMARC

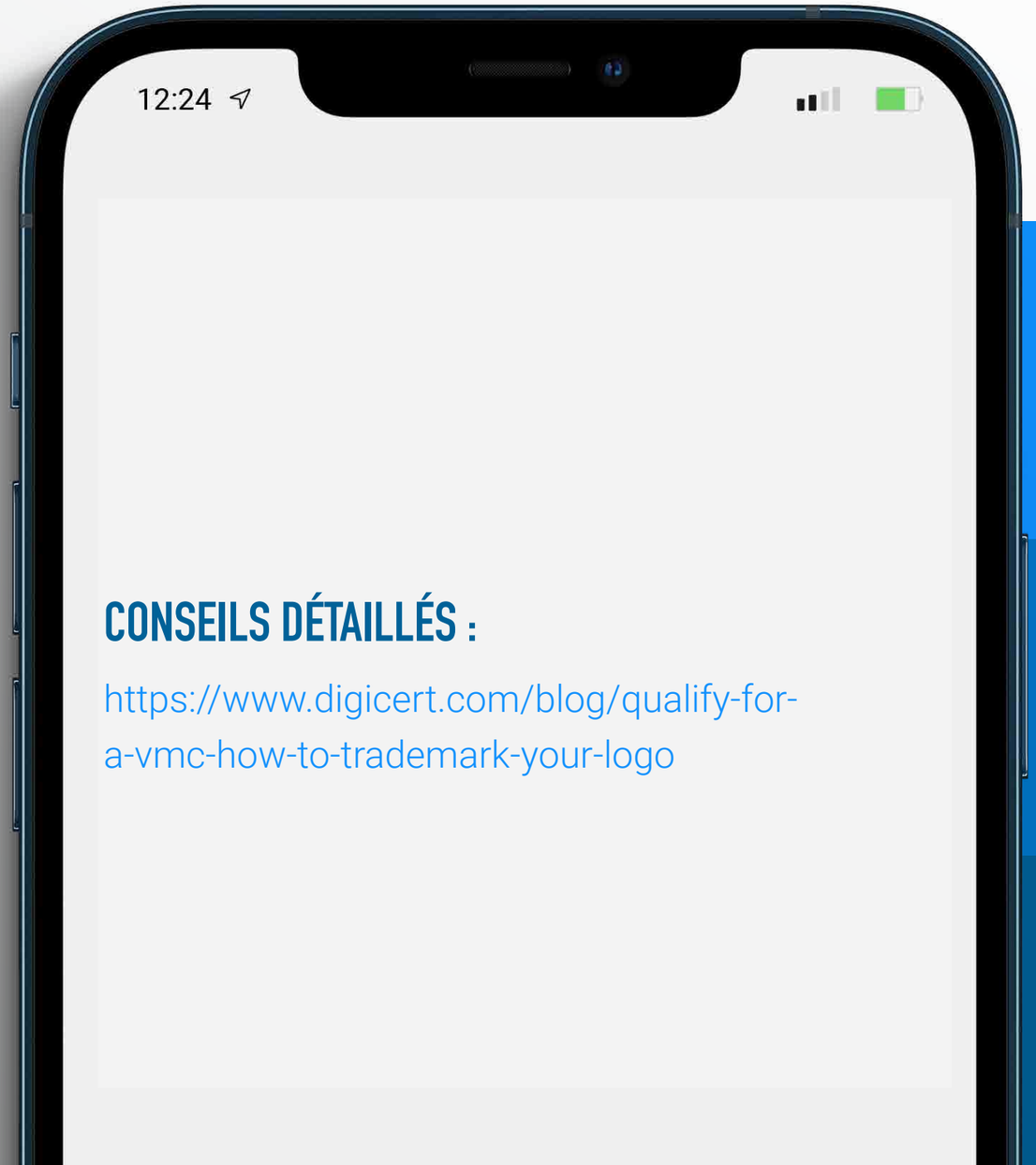
La mise en œuvre du protocole DMARC nécessite une période de test visant à s'assurer que votre entreprise ne bloque pas des messages légitimes. La durée de cette période varie selon l'entreprise, mais nous recommandons d'entamer le processus dès que possible.

MISE EN ŒUVRE DU DMARC :

https://www.digicert.com/dc/blog/how-to-set-up-dmarc-to-qualify-your-domain-for-vmc/

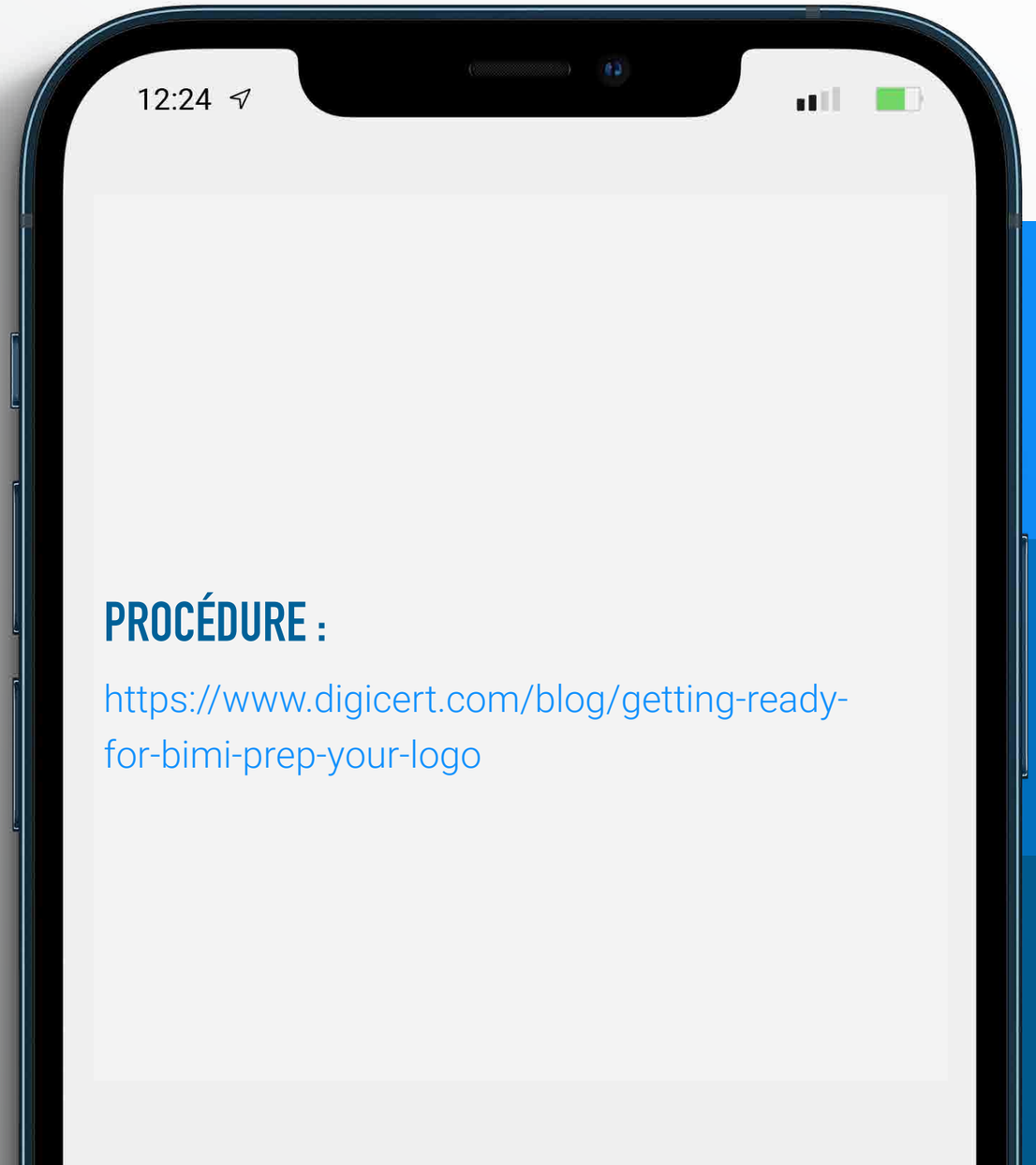
02 DÉPOSEZ VOTRE LOGO

Évidemment, le dépôt légal d'un logo ne s'opère pas du jour au lendemain. Il est pourtant essentiel car seuls les logos déposés peuvent être affichés avec un certificat VMC. Si le vôtre n'a pas encore été déposé auprès d'un office agréé BIMI, nous vous recommandons de vous rapprocher immédiatement de votre équipe juridique.



03 FORMATEZ VOTRE LOGO

Les logos vérifiés doivent être au bon format SVG pour s'afficher. Vous aurez par conséquent besoin d'un logiciel de traitement d'image et de texte.



04 ACHETEZ VOTRE CERTIFICAT VMC AUPRÈS DE DIGICERT

C’est l’étape la plus simple.
Vous pouvez vous lancer dès aujourd’hui.

MERCI

PLUS D'INFORMATIONS:

https://www.digicert.com/fr/tls-ssl/verified-mark-certificates/