



EVERYTHING IS VERIFIED. EXCEPT THE MEDIUM WE USE THE MOST.

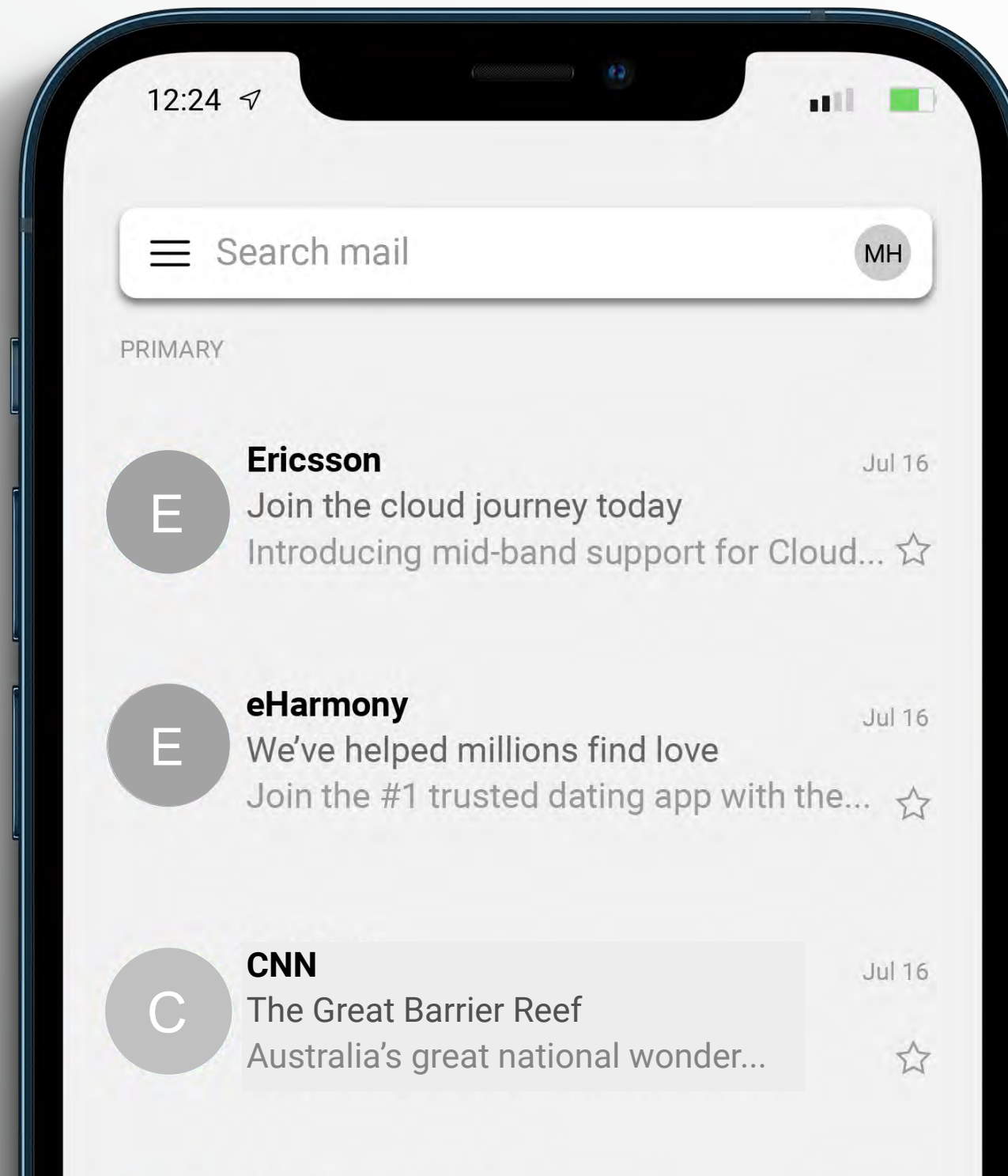
Whether it's a blue check mark on Twitter or Tiktok, a verified caller on a phone or a smart seal on an ecommerce checkout page, "verified" users and brands are increasingly common across most media. The act of verifying public accounts gives the general public an instant, concrete assurance that the person or company sending a message is the real deal. This promotes authenticity, fosters trust and provides an incentive for other users to go through the steps to verify their own account so they can stand out from the generic crowd.

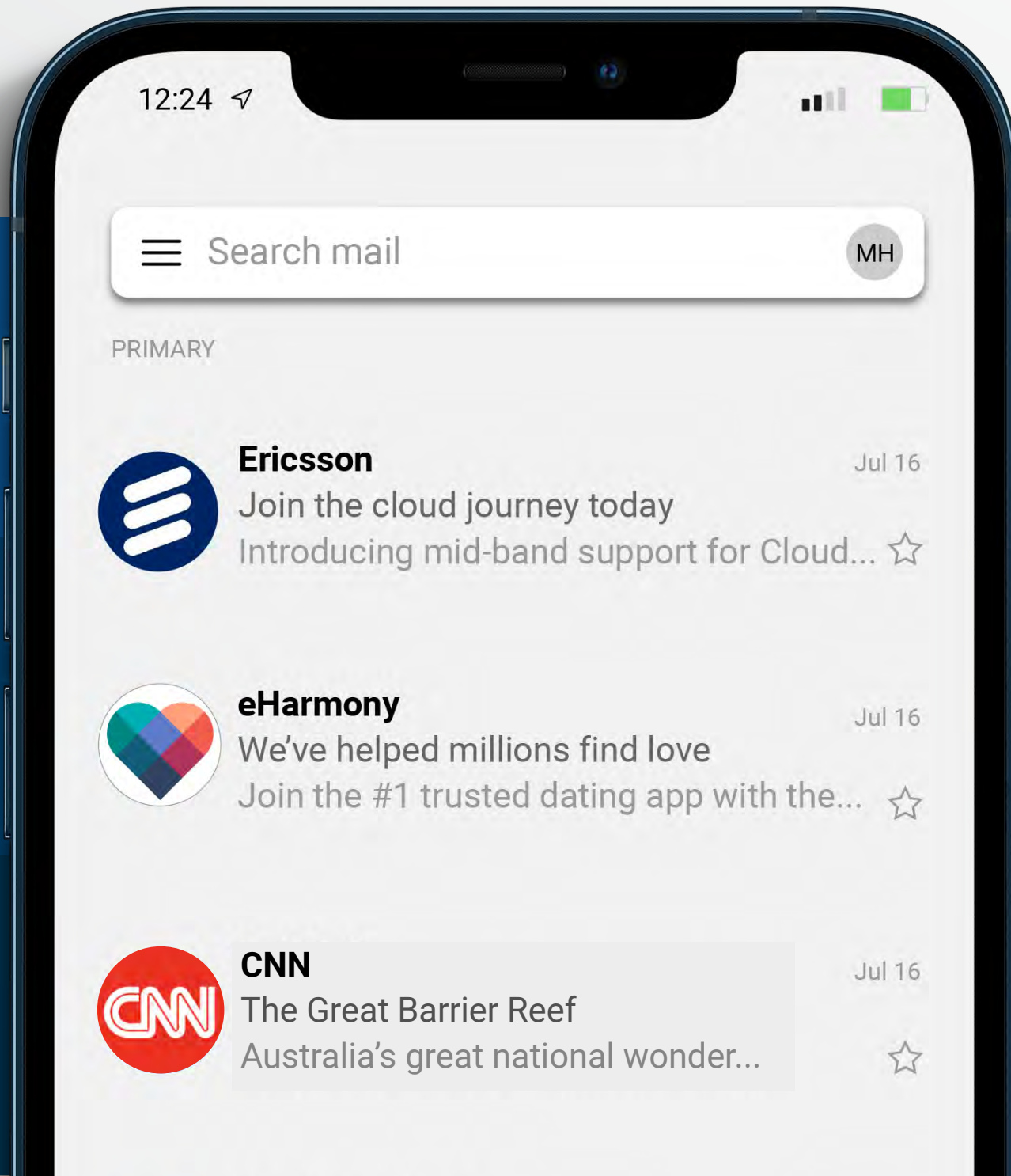




THE HUMBLE EMAIL

But for the oldest, most effective, and most widely used digital medium of all the default has long been anonymity. The unique identity of every brand and person, large or small, is reduced to a letter or two.





UNTIL NOW.



12:24 ↗



**VERIFIED MARK CERTIFICATES
(VMCS) ARE THE FIRST-EVER MEANS
OF DISPLAYING YOUR LOGO IN THE
INBOX OF YOUR CUSTOMERS—RIGHT
NEXT TO THE "SENDER" FIELD—EVEN
BEFORE THEY OPEN YOUR MESSAGE.**

IT'S TIME TO PUT YOUR MARK ON EMAIL MARKETING

Verified Mark Certificates (VMCs)—part of a groundbreaking initiative in cooperation with Brand Indicators for Message Identification (BIMI) and email client providers—are the first-ever means of displaying your logo in the customer inbox, visible to customers even before they click. And, as the last step in a series of stringent security and identity authentication measures, they help deliver greater trust and confidence in email.



MARKETING & IT. FRIENDS AGAIN.

And then there's the security component. BIMI's main goal is to incentivize brands to become DMARC-compliant, which in turn improves email security by making communication harder for attackers to spoof.

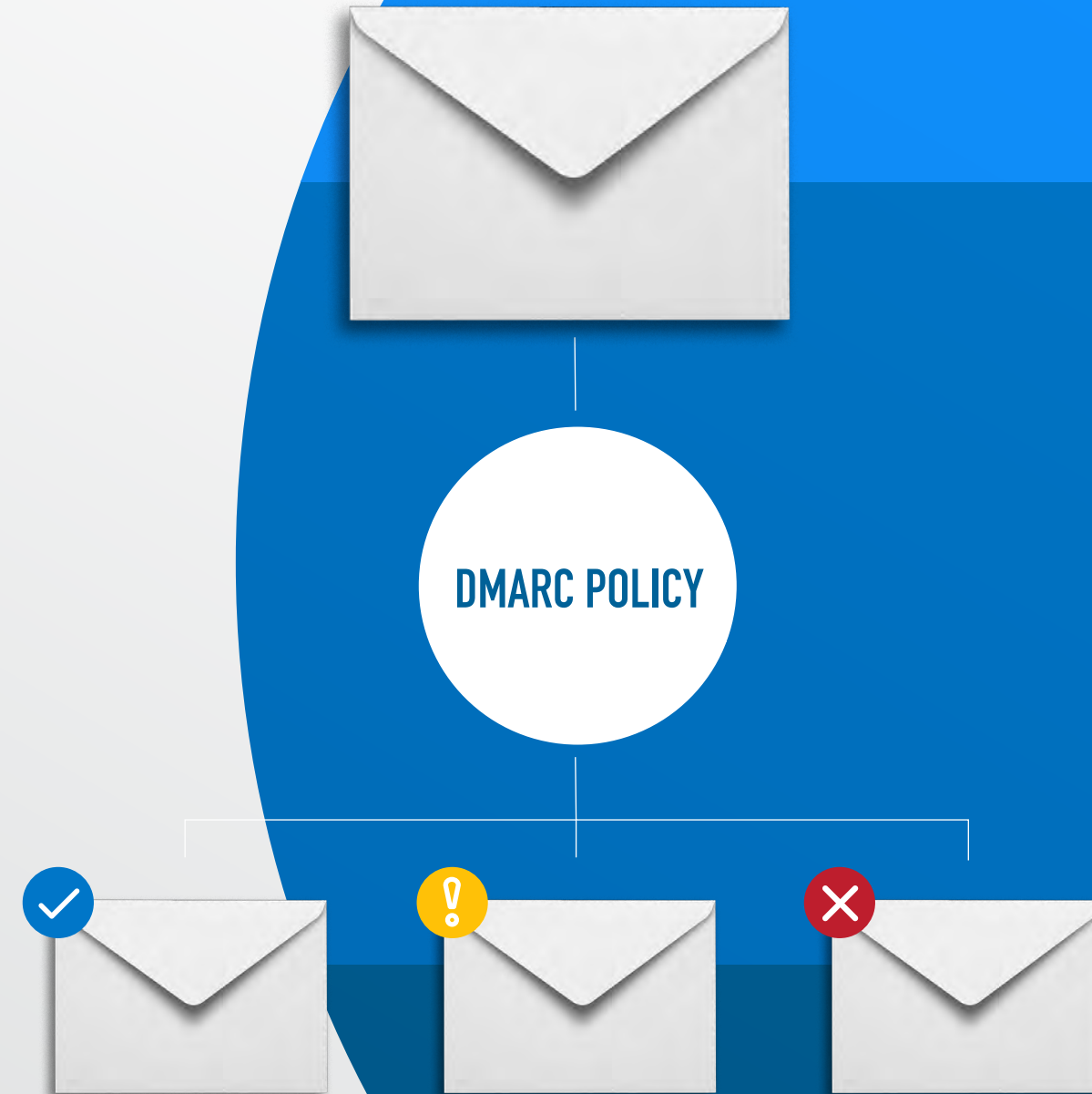
Unfortunately, despite the best efforts of IT departments around the world, DMARC enforcement remains relatively low. It's a long process, and often is put on the back burner for shorter-term, more urgent initiatives. The BIMI/VMC pilot seeks to change that by giving organizations a real-world, immediate benefit.



WHAT IS DMARC?

“DMARC, which stands for “Domain-based Message Authentication, Reporting & Conformance,” is an email authentication policy and reporting protocol. It builds on the widely deployed SPF and DKIM protocols, adding linkage to the author (“From:”) domain name, published policies for recipient handling of authentication failures, and reporting from receivers to senders, in order to improve and monitor protection of the domain from fraudulent email.”

In translation, DMARC gives security professionals more transparency and better control to accurately identify and then block or quarantine fraudulent emails more quickly. It’s a smart, commonsense standard that helps to protect both consumers and brands.



A large circular graphic with a white center and a grey-to-orange gradient border. The number "98%" is displayed in a large, bold, orange font in the center of the white area.

98%

**OF SOCIAL ENGINEERING
ATTACKS ARE DELIVERED
VIA EMAIL.**



EARNING THE MARK

A VMC-ensconced logo will display only after the email client verifies that your organization's BIMl record shows DMARC enforcement, which in turn confirms you have the tools and practices in place to help prevent phishing and spoofing attacks. The issuing Certificate Authority—DigiCert—will also check your organization's logo against your regional trademark office to make sure you're a legitimate, recognized entity, and validate the identity of the purchaser via a mobile notary. All of this adds up to indicate your organization has the right to display your verified logo.

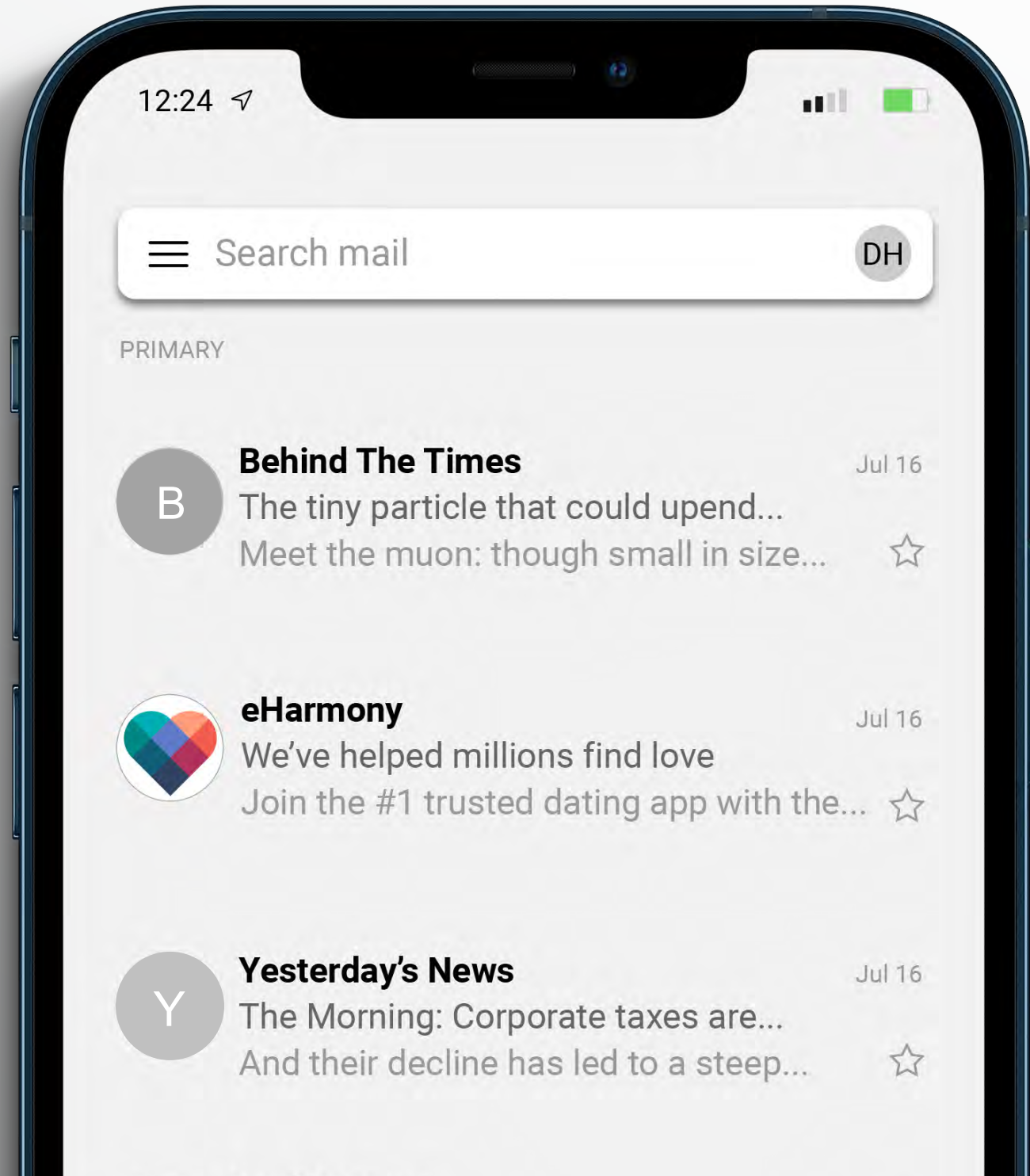
DigiCert + BIMl + VMC = Verified Email





GET A HEAD START ON STANDING OUT FROM THE CROWD.

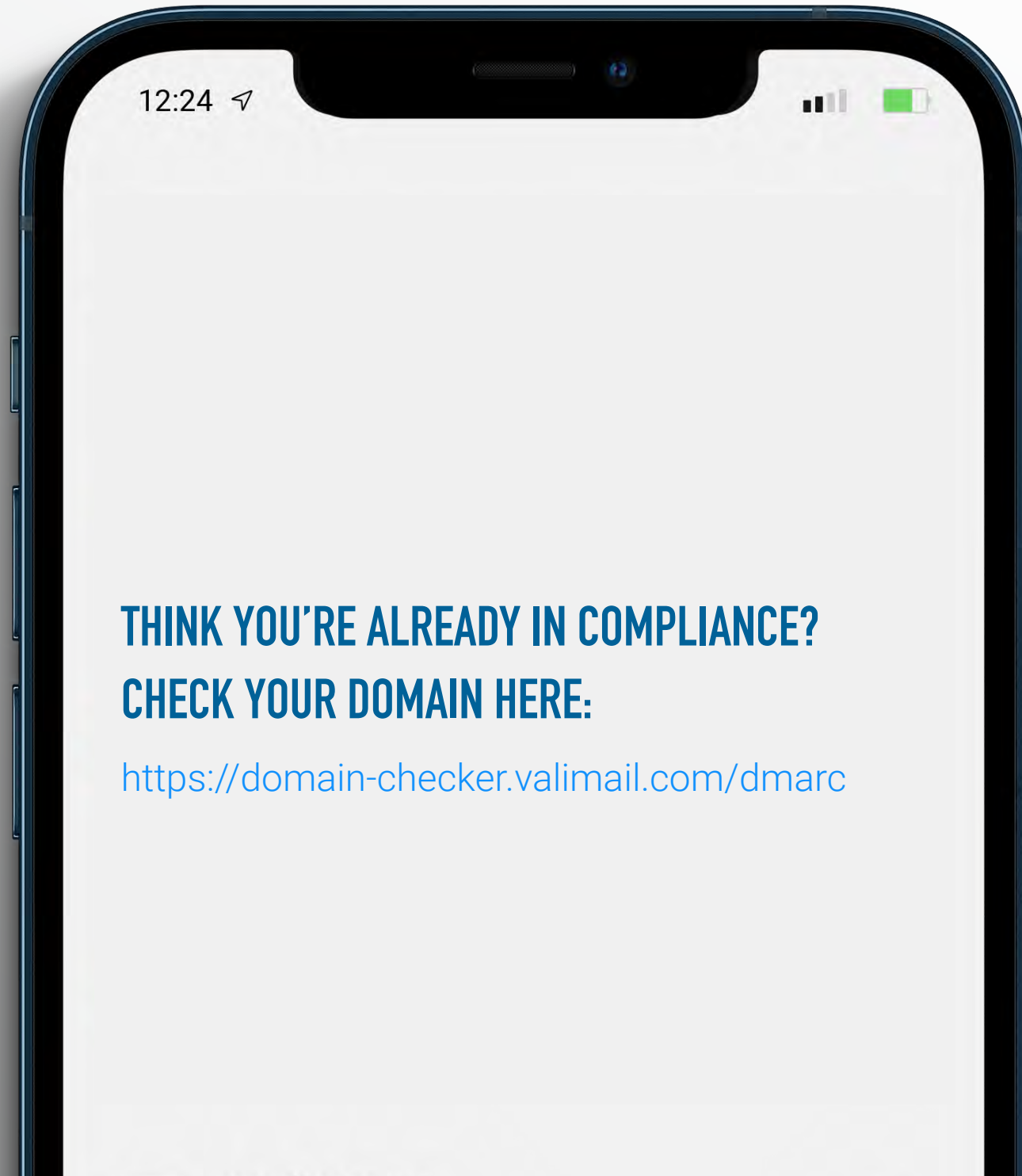
VMCs are brand new, meaning the earliest adopters have an opportunity to gain a very visual advantage over competitors. Here's how to get started.





01 ENFORCE DMARC

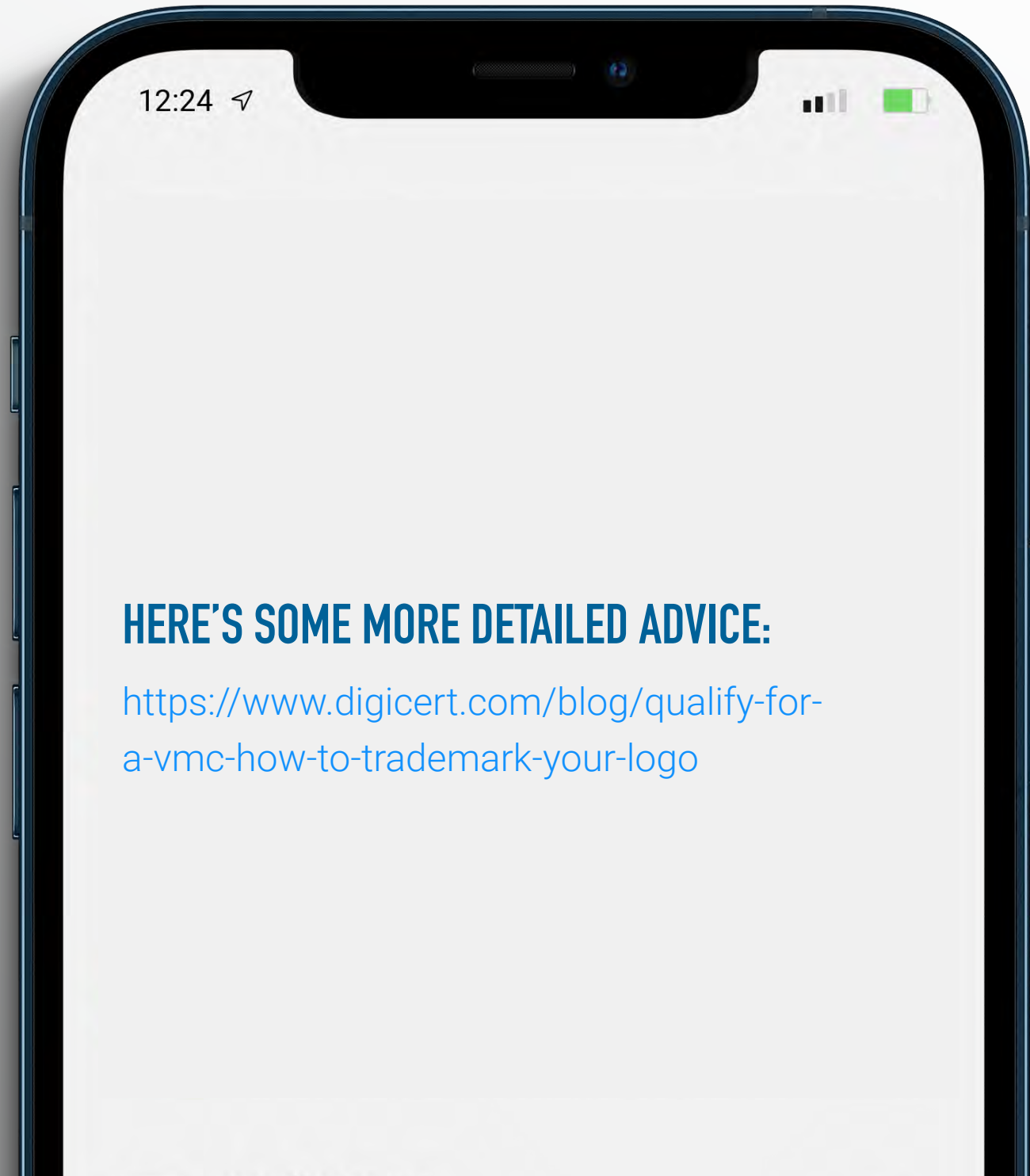
DMARC enforcement requires a period of testing to ensure your organization doesn't start blocking legitimate messages. The amount of time varies by organization, but we suggest starting the process as soon as possible.





02 TRADEMARK YOUR LOGO

Obviously this doesn't happen overnight, but only trademarked logos can be displayed with a VMC. If yours isn't registered with a BIMl-approved trademark office already, we suggest scheduling an immediate meeting with your legal team.



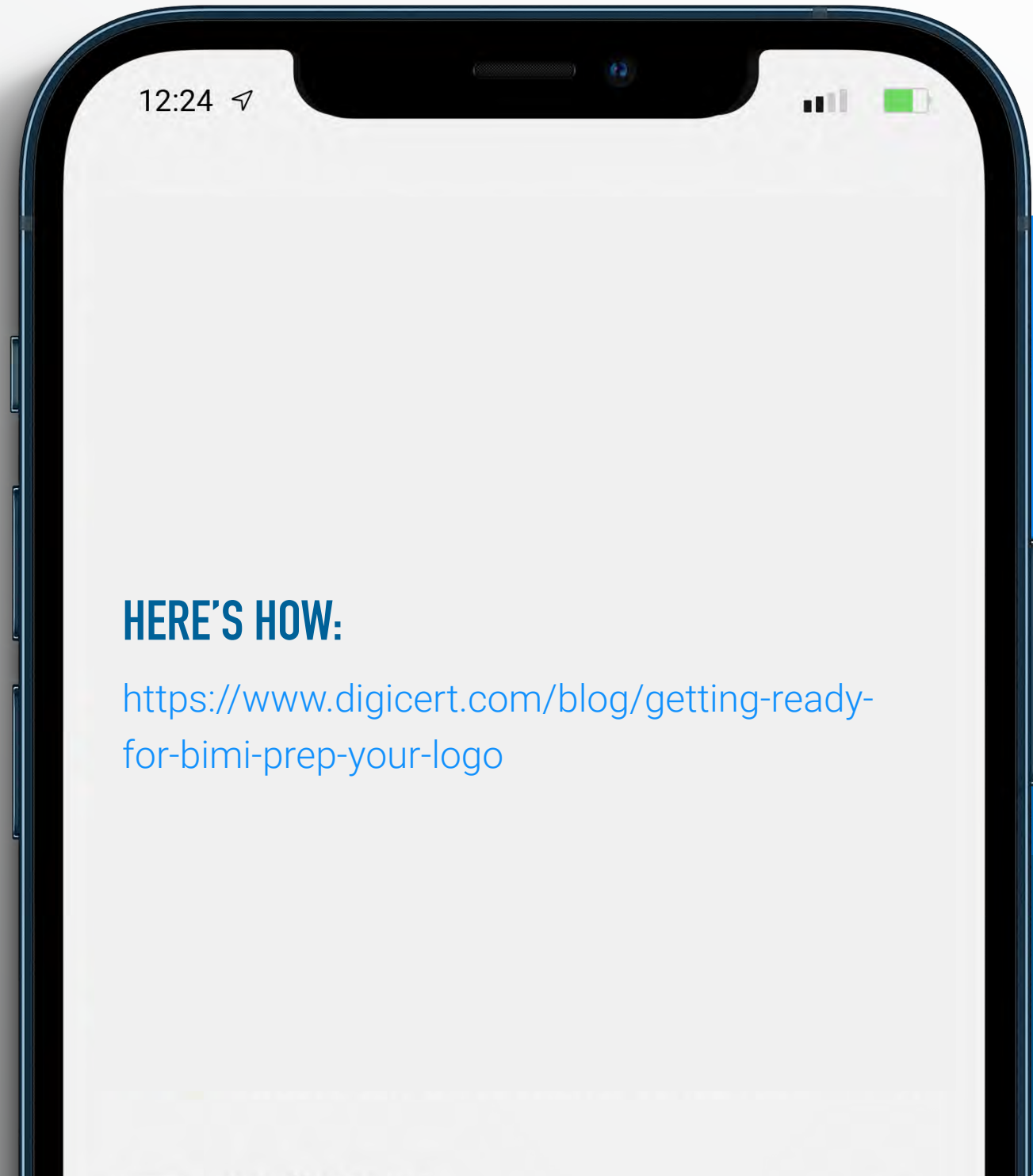
HERE'S SOME MORE DETAILED ADVICE:

<https://www.digicert.com/blog/qualify-for-a-vmc-how-to-trademark-your-logo>



03 FORMAT YOUR LOGO

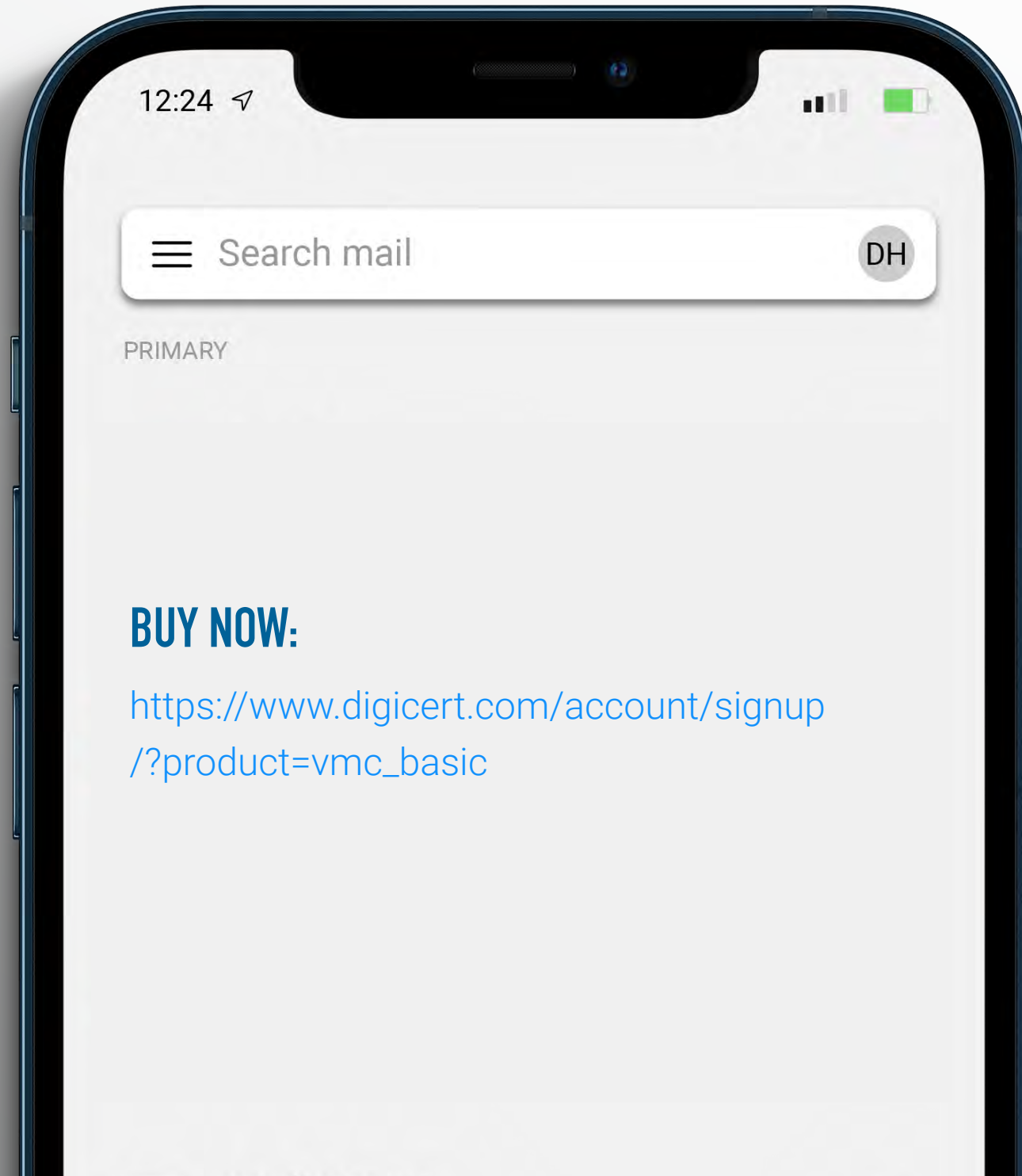
Verified logos must be in the proper SVG format to display. You'll need an image software program and a text editor.





04 BUY YOUR VMC FROM DIGICERT

By far the easiest step. Get started today.





12:24 ↗



THANK YOU

BUY NOW:

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