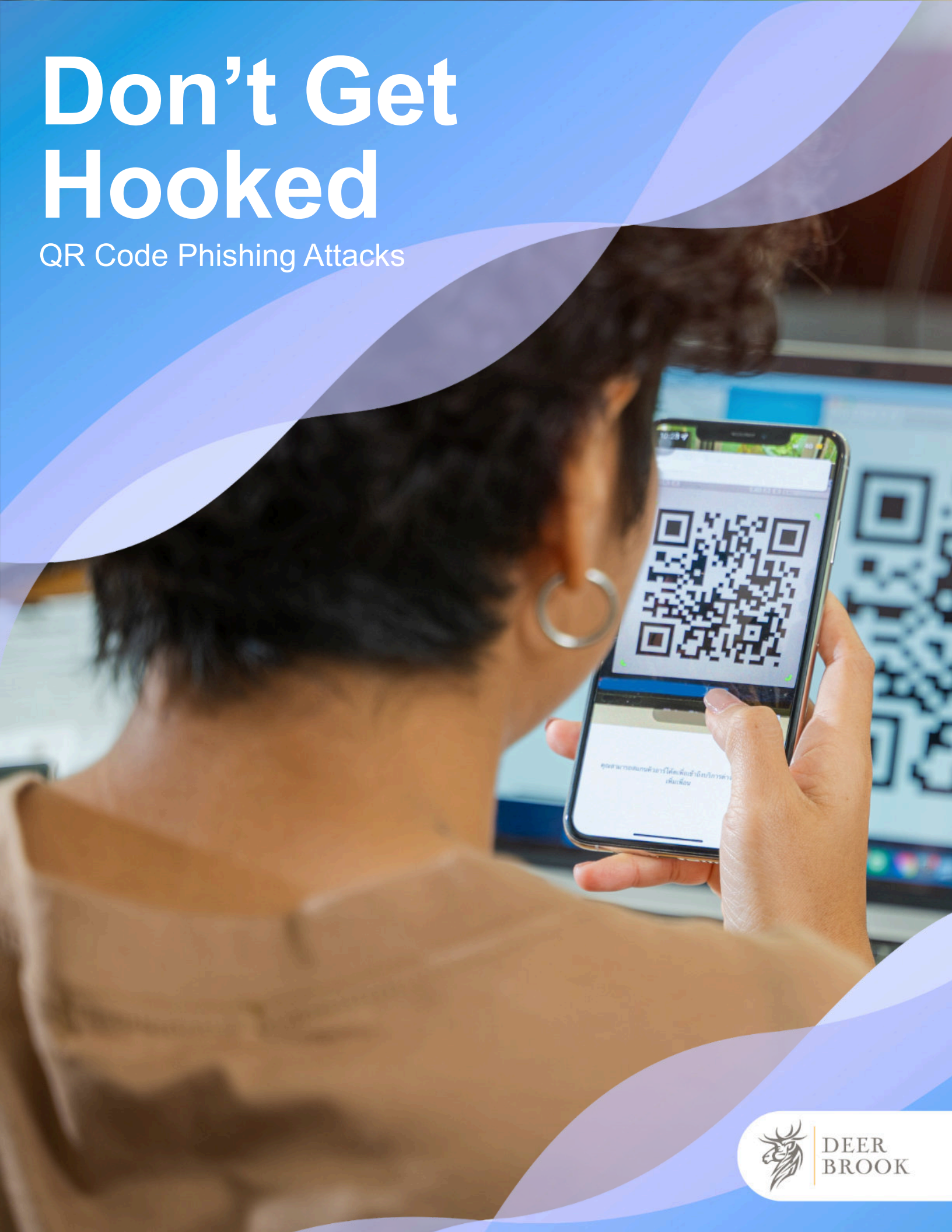
Don’t Get Hooked

QR Code Phishing Attacks



DEER BROOK

While email scams and text scams remain the most widely-known and looked out for kinds of phishing techniques, there's one less talked about but equally as devastating.

Quishing attacks are phishing attempts that make use of QR codes to conceal links and coerce victims into handing over their personal information, download malware, or both.

What are QR codes?
You've probably seen QR codes out in public; they're usually square black and white images that look like barcodes. QR codes can direct users towards all sorts of things once they're scanned: QR codes can redirect users to URLs, prompt them to send an email to a specific person, and can contain data like network information, Wi-Fi passwords, serial numbers, and more.

Ultimately, QR codes are a quick and easy way to direct users towards something. That's why legitimate QR codes are often sent through email threads, text threads, and are posted in public places like restaurants and bulletin boards. However, malicious QR codes are often leveraged in the same exact ways as part of phishing cyberattacks.

What makes QR codes dangerous?

First things first, QR codes themselves aren't dangerous. Rather, it's the way bad actors can leverage QR codes that gives them their potentially dangerous edge.

Hidden by nature
Unlike a URL, there's no way to quickly check the details of a QR code to verify it takes you where it says it does. To the human eye, all QR codes are alike.

In phishing attacks, malicious QR codes often lead victims to spoofed websites with malware. From there, the threat actors can use a myriad of techniques (some automated, some interpersonal) to attempt to steal sensitive data like passwords and credit card information.

How do quishing attacks get through?
When the QR code isn't just being posted in public, preying that curiosity gets the best of someone, quishing attacks are still trying to leverage the convenience of a potential victim's phone.

Generally speaking, phones and mobile devices aren't as well-protected as computers and workstations, especially those used for work and those connected to a company's network. In a work context, this makes QR codes very dangerous as an attack vector, especially in company environments where employees bring their own devices.

Masquerading as official companies
Scammers will often trick victims not by coercion, but by impersonation. QR codes leveraged in phishing scams often direct victims to fake Microsoft 365 login portals to harvest their credentials. Once stolen, those credentials are then used to take over a user network account.

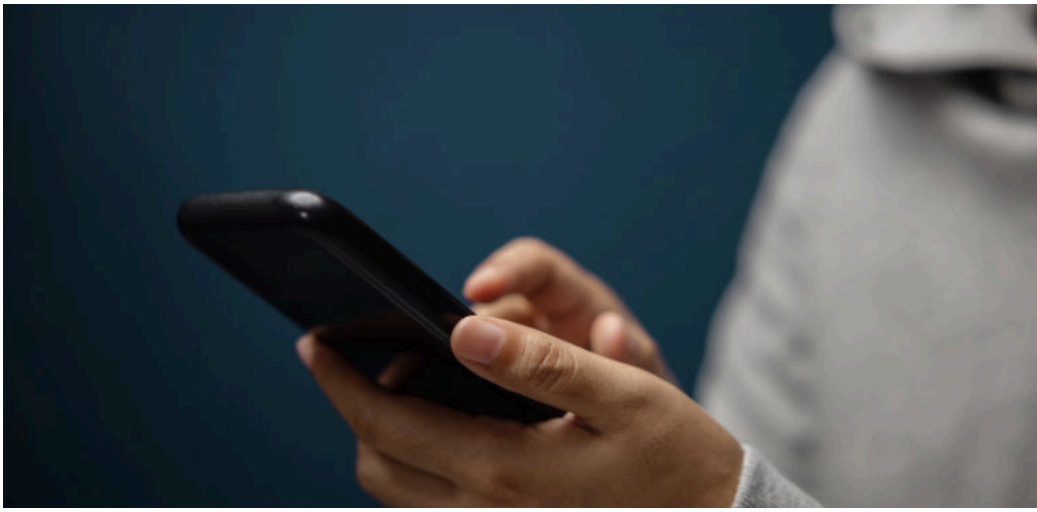
The same flavor of scam tries to steal users' personal, non-work information too. Phony QR codes for banks, government services, mail delivery and more, have all been circulated at one point or another.

How can you spot a quishing attack?

QR code phishing attacks don't often drop a sole QR code and leave it at that. Often, they come bundled as part of an email, text, or other notification that's designed to capture your attention.

Be skeptical
To grab your attention, scammers will often try and create a compelling narrative about an important service you use often that contains your personal information.

Be on the lookout for messages about invoices (especially with an attachment), requests for personal information, and reports of



suspicious activity on an account you might have.

Other subjects that have proven popular for quishing are government refunds, coupons and discounts on products and services, and calls to make payments (especially being labeled as "late" payments).

If you come across any of these kinds of messages directed towards you, steer clear if they include a QR code, links, or any other sort of attachments.

Other ways to defend against QR code attacks

Don't scan QR codes found in the wild
While it's not often you'll find a rogue QR code in public, just play it safe and don't scan any codes you see while you're out and about.

You don't know who put it there, and you'll never know their intentions why. It's best to just ignore it and move on.

Be suspicious
If you scan a QR code and are led to a website that asks for your password or other login information, put your plans on hold. Verify the website's details before moving forward.

Play it safe
In general, don't scan QR codes you receive through email or text, unless you know for a fact they're legitimate. When you're not sure, call the sender to confirm the code's authenticity.

Put on your investigator's hat
Some scammers have taken to pasting malicious QR codes over legitimate ones on physical and digital advertisements.

If it looks as though a QR code has been tampered with in any way, do not scan it. The same caution applies to flyers and materials you might receive yourself, such as through the mail.

Don't get caught by a quisher
Ultimately, email scams and text scams are more widely known than QR code scams for a reason; they're far more popular as attack vectors and therefore need more awareness.

However, that's not to downplay the seriousness of quishing and QR code attacks. They can be just as dangerous as any other phishing scheme when it's all said and done.

As with all phishing attacks, the best defense is to think defensively from the onset. Always be skeptical when you receive messages and alerts you weren't expecting, and double-check the authenticity of any links you're asked to click on. Do not open any attachments.

For scammers, victims are just another number. Be active and alert, and turn attempted quishing attacks into just more failed scams instead.