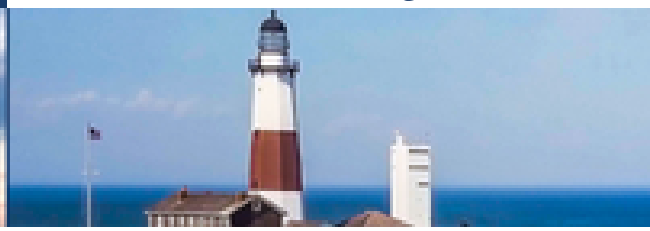
CYBERSECURITY AND DATA PRIVACY LAW ALERT
February 26, 2024
By: Andrew T. Garbarino, Esq.
Richard M. Frankel, Esq.

RUSKIN MOSCOU FALTISCHEK P.C.
Smart Counsel. Straight Talk.



Why You Should Be Concerned With "Quishing"

Be careful the next time you scan a quick response (colloquially known as a "QR") code, because it may open your device to a bad actor.

Despite being a fairly old technology – they were first developed in the mid-90's – QR codes rose to prominence with the advent of smartphones. The use of QR codes skyrocketed during the pandemic as restaurants and other business moved towards contactless options for customers. QR codes won't be vanishing any time soon; 99.5 million Americans are predicted to use QR codes by 2025. See Rebecca Kowalewicz, "Marketing With QR Codes", Forbes, September 21, 2022, here.

Standing as yet another indication that cybercriminals are becoming increasingly sophisticated, bad actors are now exploiting QR codes to gain access to smartphones and similar devices – a scheme called "quishing". The Federal Trade Commission's guidance on the use of QR codes to scam individuals may be found here.

The unfortunate term for this scam aside, considering the ubiquitous nature of QR codes on restaurant menus, parking meters and even in courthouses, this scheme is especially insidious as people have simply gotten used to scanning a QR code at a business. Placing a sticker over an existing QR code is far easier than attaching a device to an ATM card-port.

RMF has at least one client who suffered multiple fraudulent charges within just a few minutes of scanning a QR code. He was thankfully notified of the charges by his bank.

Just as one should think before they click on a link, one must think before scanning a QR code. Looking for similar indicators, such as misspellings, slightly altered company names and other unusual features associated with the code may be a crucial tip-off.

Likewise, don't engage a QR code that is texted to you without verifying the sender first.

Finally, as always, keep your devices current with the latest security updates as technology companies continue to grapple with the logistical issues attendant to combatting cyber criminals.

For more information, please contact:

Andrew T. Garbarino, Esq.
516.663.6632
agarbarino@rmfpc.com

Richard M. Frankel, Esq.
516.663.6534
rfrankel@rmfpc.com