BANK OF AMERICA

Be cyber secure: click safely

Links and QR codes are everywhere. From your favorite news site to your social media platform of choice, companies want to direct you to their content and products. Unfortunately because legitimate companies use these tactics, so are cyber criminals.

Here are some best practices to utilize when clicking on links to make sure they are safe:

QR Codes: Quick Response codes are a type of barcode that, when scanned, will take you to the information it contains.

- See whether the QR code has a preview mode.
- Ensure that the source of the QR code is a reputable, trusted source.
- Inspect the QR code to check that it has not been tampered with in any way, for example, check to see if someone has placed a different QR code over the top.
- If in doubt, go directly to the source of information, do not scan the code.

Shortened links: a way of making a URL smaller while still directing those that click on the same web page. Ensure you are clicking on shortened links safely:

- See whether the shortened link has a preview mode.
- Research the shortened link you are trying to use and see whether they have verification methods.
- Ensure that the link is coming from a trusted, reputable source.
- If in doubt, go directly to the website you want to browse, do not click on the link.

Here are some tips that can help protect you from malicious links and QR codes or prevent you from taking action that could be costly:

- **Make sure you only click on links from trusted sources,** and if you are on social media channels, look for verification check marks to confirm the channel is legitimate.
- **Use caution** when encountering shortened links or QR codes, and ensure they are from trusted, reputable sources.
- **Update all operating systems, apps, and security software** — including antivirus programs and firewalls.
- **Don't fall for the bait.** If an offer sounds too good to be true, it probably is. Or if an email looks strange, look up the sender and call them using a known and trusted number.
- **Remember** that Bank of America, like many businesses, will never ask you for account or details unless you call us first.
- If you have been targeted, **report** the incident to local law enforcement immediately and contact your bank.

Visit www.bankofamerica.com/security-center/overview/ to learn how to help protect yourself and those closest to you.