Huntington Welcome.®

Tips to Help Avoid Coronavirus-related Scams

As the Coronavirus (COVID-19) epidemic continues to escalate, cyber criminals are taking advantage of opportunities to steal personal and financial information while people are frightened and most vulnerable. Many of these instances are new iterations of common phishing and malware scams, where fraudsters may send emails with malicious attachments or links to fraudulent websites to trick victims into revealing sensitive information or donating to fraudulent charities or causes. Fraudsters may use phone calls (vishing) and texts (smishing) to try to trick you as well.

What to look out for

Be extra vigilant when receiving emails, phone calls and texts offering vaccines or treatments, medical testing or alerts about critical supply shortages. Fraudsters are also spoofing the World Health Organization (WHO), Centers for Disease Control and Prevention (CDC) or other similar medical, charitable and government organizations. These messages can be highly convincing, as cyber criminals often use professional "phishing kits" that perfectly match the logo, website and email formats of legitimate organizations.

If you do receive unsolicited phone calls, emails or text messages asking you to share personal, financial or account information, verify the request using an alternative method before taking any action. Locate the entity's phone number from a trusted source, such as their secure website or a recent bill or statement, or the back of your credit or debit card if the caller is purporting to be from your bank. Use that phone number to call back to verify that the caller and the reason for the call are legitimate.

What you can do to help protect yourself

Tips for emails:

- Look closely at the sender's email address and domain. Check for misspellings and inconsistencies between the "Sender" name and "From" email address or domain name—or if the email originates from a non-corporate email address (ex. Gmail)
- Beware of demands for personal or financial information, especially those with a sense of urgency.
- Be extra cautious before clicking any links in the email. You can preview links to see where they go by hovering your mouse over the link without clicking on it. It will display the real website address.
- Pay attention to links and web addresses as a spoofed website can be similar to a recognized entity, but are off by one or two characters. Do not assume it is legitimate because it displays a corporate logo.
- Do not open attachments from sources you do not recognize
- If you receive a suspicious email claiming to be from Huntington, please let us know by forwarding the email to ReportFraud@huntington.com.

Tips for phone calls:

- Ignore telephone numbers that are in a strange or unexpected format, or are from an unfamiliar location.
- Even if the call is from a recognized entity, remember that scammers sometimes utilize Voice over IP (VoIP) features, such as caller ID spoofing and automated systems, to help mask where the call is coming from.
- If you receive an unsolicited call, before providing any personal or financial information, tell the caller you will call them back and use the verification method described above to confirm the caller and the reason for the call is legitimate.

Tips for text messages:

- Avoid clickingng links in unsolicited text messages from unknown numbers.
- Do not direct dial any phone numbers listed in unsolicited text messages from unknown numbers.
- If a text message requests for personal or account information, do not respond. Use the verification method described above to confirm the requester and the reason for the request is legitimate.
- Be wary of messages that offer you free or scarce items or demand an urgent response. If it seems to good to be true, it usually is.

How Huntington can help

Certain Huntington checking accounts include access to credit score and/or identity monitoring[1] at no added cost. Learn more about these services and how to enroll at **huntington.com/help-protect-yourself.**

Visit **huntington.com/Security** for more tips on protecting yourself and to learn more about how we help protect your privacy and keep your information secure.

If you think you may be a victim of fraud related to your Huntington credit or debit card, or your card has been lost or stolen, please let us know right away at **(800) 480-2265.**

[1] The Monitoring Services are optional and are not available with all accounts. Enrollment requires agreement to the Services' Terms & Conditions, which include important legal terms that a customer should read carefully before deciding to enroll.

13351-C | 03/20