

Learn to spot phishing scams

Legitimate companies will not ask you to provide or verify sensitive information through non-secure means, such as email or text.

Posing as legitimate companies

- ❑ Email and web addresses that are similar to a recognized entity, but are off by one or two characters.
- ❑ Ask for information that they should already have: your account number, Social Security Number, Employer Identification Number, or username and password.
- ❑ Be cautious if they refer to recent activity that you didn't make, such as a purchase or deposit, or to an account you don't have.

Messages that create a sense of urgency

- ❑ Claim there has been suspicious activity on your account.
- ❑ Indicate a loss of access to your account if you don't respond.
- ❑ Request you upgrade or install new privacy software or identity theft solutions.
- ❑ Offer a gift or prize for responding.

Emails with links or attachments

- ❑ Include web links that at first glance look right, but lead to a fraudulent website.
- ❑ Attach a document that looks legitimate but contains malware (malicious software). Only open attachments you are expecting to receive.
- ❑ 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.

Know when you may have been phished

- ❑ Your statements stop being delivered to your current address.
- ❑ Suspicious charges to your account.
- ❑ Denied credit unexpectedly.
- ❑ IRS notification of duplicate taxes.

Tips to help protect yourself

- ❑ **Enroll in Huntington Online Banking (if you haven't already).** Regularly sign in to monitor your accounts.
- ❑ **Use Huntington's Mobile app.** The Quick Balance feature allows you to quickly view your balances.
- ❑ **Sign up for Huntington alerts.** Set up email and text alerts¹ to be aware of activity/transactions.
- ❑ **Do not provide your Social Security Number unless absolutely necessary.** If you must provide your Social Security Number, call a known phone number or ask for them to send a written request through the mail.
- ❑ **If you receive a call or email you did not initiate requesting personal information, ask them to send you a written request.** If they refuse or you are not comfortable with the phone call, tell them you're not interested and hang up.
- ❑ **If your account statement does not arrive as expected, contact Huntington immediately.** A missing statement could mean an identity thief has taken over your account and changed your billing address to cover their tracks.
- ❑ **Be careful what you post online about yourself.** Understand your online privacy settings for social media and websites you visit.
- ❑ **Check your credit report regularly.** The law requires each of the national consumer reporting agencies to provide you with a free copy of your credit report, at your request, once every 12 months.

Contact Huntington

If you receive a suspicious email, call or text claiming to be from Huntington, let us know. We'll work with you to determine the legitimacy of suspicious messages and account activity.

PHONE: **(800) 480-2265**

EMAIL: **ReportFraud@huntington.com**

For more information about phishing, go to **huntington.com/Phishing**.

¹Carrier's message and data charges may apply.