Huntington Welcome.℠

Fraud is on the rise. Scammers are getting smarter. Help protect yourself from phishing scams.

HOW PHISHING SCAMS WORK

Phishing scams are attempts by someone to deceive you into disclosing personal or financial information that they can use to steal your money, identity or both. Attempts come through emails, phone calls and texts, and target all ages, all income levels, and businesses as well as individuals.

By posing as someone you know, or as a legitimate company such as your bank, the fraudster asks you to provide or verify personal information such as a Social Security Number, account numbers and/or password/login information.

Phishing scams usually have two things in common: 1) they create a sense of urgency to get you to respond; and 2) they ask for information they should already have.

PHISHING SCAMS USUALLY TAKE THREE FORMS:

Email (Phishing)
Designed to look legitimate, these emails trick you into giving out personal or financial information, or clicking on a malicious link.

Phone (Vishing)
The caller claims to be from a bank/IRS or asks for personal or financial information to help a family member or friend in trouble.

Text (Smishing)
Texts (SMS messages) can appear to be from a person or company you know to trick you into clicking a link or texting back personal information.

Remember: Huntington will never ask you for account numbers or passwords by phone email or text.

Beware Fake Mobile Baking Apps

Fraudsters may develop and publish fake mobile banking applications designed to look like an official Huntington Mobile Banking app in order to collect personal information, including username/password, with the goal to commit identity theft or account takeover.

The Huntington Mobile App is only available from the Apple App Store (iOS) and Google Play (Android). Any mobile apps advertised on third-party sites should not be used downloaded. The developer or author of the application is Huntington National Bank.

HOW TO PROTECT YOURSELF

At Huntington, protecting your personal and financial information is a top priority. The checklists on the next page can help you spot and protect yourself from phishing scams.

1.2 million
phishing attacks in 2016 (up 56% from 2015) [1]

97%
of people can't identify a phishing email [2]

1 in 131
emails contain malware (malicious software) [3]

#1
type of phishing lure is email with a fake invoice [3]

12%
of people click malicious attachments or links [4]

1 Source: APWG Q4 2016 Phishing Activity Trends Report
2 Source: Intel Security Phishing Quiz Findings
3 Source: Symantec 2017 Internet Security Threat Report (ISTR)
4 Source: 2016 Verizon's Data Breach Investigations Report (DBIR)

The Huntington National Bank is an Equal Housing Lender and Member FDIC. ®, Huntington® and Huntington. Welcome® are federally registered service marks of Huntington Bancshares Incorporated.

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 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 alerts† 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.

† Carrier's message and data charges may apply.