

## **PHONE PHISHING – Information from Huntington Bank**

As you may know, “phishing” refers to the efforts of scammers and con artists who try to fool you into revealing personal information or sending money. Although the term is frequently associated with internet scams, there has been a tremendous upsurge in phishing by phone.

### **1. How to spot a phone phishing scam**

The most effective scams tend to play upon strong emotions:

- Empathy – “You have a relative in financial trouble.”
- Fear – “Your assets are about to be seized by the IRS.”
- Excitement – “You’ve won a drawing for a new house.”

Other popular scams making the rounds:

- News of government grants you can collect – “We just need your social security and deposit account numbers.”
- Calls from technology companies who claim they can fix a serious security breach on your computer – “Your access codes, please.”

And scammers almost always try to pressure you into making an immediate decision:

- “You have to act immediately, or your credit card will be shut off.”
- “Only the first five people we call who say ‘yes’ will get this free vacation.”

### **2. Follow these basic safety rules to guard against phone phishing**

Just remember, **all of these common schemes are designed to get one of two things: your money or the passwords and other data that can be used to get your money.** The instant you hear that request, it’s time to slow down, get suspicious, and verify the claim or offer.

- Never conduct business with anyone online or over the phone unless you can confirm their identity, preferably by re-contacting them using a phone number or email address you locate independently.
- The caller may claim to work for a company you trust. They could know personal information about you, to better impersonate a representative from that company. Even the Caller ID on your phone is not proof that the call is coming from a legitimate business.
- If anyone asks you for money or personal data, do the safe thing: say no and hang up.

### **3. Become a scammer's worst nightmare**

Start reporting scams you encounter to the Federal Trade Commission. You can file a report online at the FTC website or by calling (877) FTC-HELP.

Finally, spread the word about phone phishing. By keeping friends and loved ones informed, we can work together to limit the damage phone phishing tactics can inflict on all of us.