Haverhill Bank
Just One Bank

Business Security Newsletter
Issue 6 – Spring 2019

Government Imposter Scams

Today's businesses have to defend against various types of fraud, including government imposter scams. These scams occur when fraudsters try to intimidate victims into sending money or sharing account information by posing as a trusted government agency.

Types of Government Imposter Scams

The key to a successful government imposter scam is to invoke a sense of fear and urgency in the victim. Typical government imposters will claim to be calling on behalf of a trusted state or federal agency and will present you with a variety of scenarios, including:

- Telling you that you owe thousands of dollars in back taxes to the IRS
- Threatening that you'll lose your trademark if you don't pay a fee to the U.S. Patent and Trademark office
- Offering a fake government grant to assist with business expenses if you provide your checking account information

These actors may create a sense of urgency by threatening arrest or massive fines if the payment is not made immediately. They'll likely ask you to make payment in the form of a prepaid debit card or wire transfer.

How to Protect Your Business

- **Don't trust a name or number**. With advances in technology, con-artists are able to easily manipulate the name and number that shows up on your caller ID. If you think a call from a government agency is legitimate, call them back at a known number.
- **Don't wire money or share account information.** A legitimate government agency will not require a specific type of payment and will never ask for your account number or other financial information.
- **Be aware of the point of contact**. Government agencies will typically contact you via mail, not email or via phone.

#TechTips for business owners

Safeguard your network by requiring a strong password to gain access to your company's wi-fi. For added security, set up your wireless router so that it does not broadcast the system's name, making it harder for criminals to identify.

Set up individual user accounts for your employees, allowing them to access only the data systems they need to help keep confidential customer and business information secure.

Educate your employees about cyber crime and teach them about the preventative actions they can take to protect your business.

For more Tech Tips, visit the Security page at haverhillbank.com