HANOVER POLICE DEPARTMENT
46 LYME ROAD, HANOVER, NH 03755
(603) 643-2222
Charles B. Dennis, Chief of Police

MEDIA RELEASE

Hanover Police are informing community members to be aware of email scams targeting businesses. In these email scams, hackers will forge their email address and assume the identity of someone within the organization, typically in management. They will then send the forged email to someone with the authority to make a payment, such as a finance director, asking that a payment be made to someone, for example a "new vendor".

Many of these emails will have follow-up emails asking you about the status of the request. In many cases the emails are so convincing that the well-intentioned recipient will send the money without hesitation. These hackers are doing their homework on organizations they are targeting.

Please be aware of who is calling you and emailing you. If someone is contacting you and wanting you to send money or requesting personal information, be suspicious. Two things that you should do before sending out personal/sensitive information or completing any wire transfers are:

1. Call the supposed sender to verify that the email is legitimate; or
2. Start a separate email chain with the sender asking if they did in fact request that information.

These extra steps could save you or your business from making bogus wire transfers. Lastly, trust your gut instinct when it comes to these types of emails. If it doesn't feel right, check it out further.

I have attached to this release an article from the Federal Trade Commission on imposter scams.

Issued By: Charles B. Dennis, Chief of Police

Date: November 27, 2017

Time: 1:00 PM

have you HEARD about...

Imposter Scams

Here's how they work:

You get a call or an email. It might say you've won a prize. It might seem to come from a government official. Maybe it seems to be from someone you know – your grandchild, a relative or a friend. Or maybe it's from someone you *feel* like you know, but you haven't met in person – say, a person you met online who you've been writing to.

Whatever the story, the request is the same: wire money to pay taxes or fees, or to help someone you care about.

But is the person who you think it is? Is there an emergency or a prize? Judging by the complaints to the Federal Trade Commission (FTC), the answer is no. The person calling you is pretending to be someone else.

Here's what you can do:

1. **Stop. Check it out – before you wire money to anyone.** Call the person, the government agency, or someone else you trust. Get the real story. Then decide what to do. No government agency will ever ask you to wire money.

2. **Pass this information on to a friend.** You may not have gotten one of these calls or emails, but the chances are you know someone who has.

Want to know more? Sign up for scam alerts at ftc.gov/subscribe.

...Pass it ON

Please Report Scams

If you spot a scam, please report it to the Federal Trade Commission.

- Call the FTC at 1-877-FTC-HELP (1-877-382-4357) or TTY 1-866-653-4261
- Go online: ftc.gov/complaint

Your complaint can help protect other people. By filing a complaint, you can help the FTC's investigators identify the imposters and stop them before they can get someone's hard-earned money. It really makes a difference.