Bahl&Gaynor
Investment Counsel

March 4, 2021

COVID Complications: Identity Theft

By Glenn Warden, *Chief Information Officer,*
Bahl & Gaynor Investment Officer

The global pandemic is spawning another sweeping and insidious issue, **identity theft.** The Federal Trade Commission received nearly 28,000 fraud reports related to COVID-19, often tied to unemployment benefits and stimulus payments. The FBI's Internet Crime Complaint Center reports a big rise in COVID related phishing scams. Interpol, working with ID verification experts, found global fraud rates increased by 41% over the previous year[1].

Fake emails including links to COVID information from what appear to be known sources (i.e. Centers for Disease Control and Prevention) might seem helpful, but by clicking on the link you may unknowingly download malware to your device, compromising it and your personal information. Don't be deceived by people pretending to be contact tracers, asking for your Social Security number or even a payment for tracking services.

Phishing scams are, of course, not new. The pandemic simply provides more opportunity for fraud. Now, with tax season in full swing, impersonators have yet another way to violate your privacy.

Bahl & Gaynor offers our clients instructions to follow should they believe they are victims of identity theft. We're happy to share... you'll find them in our Resources. Yes, we are increasing our reliance on electronic communication; the last thing we need is increased risk of fraud. Now, more than ever, let's protect ourselves from another COVID complication.

Things you can do to protect yourself from identity theft:

- Freeze your credit with all the major credit bureaus: Equifax, Experian and TransUnion. It's free, doesn't affect your credit score, and prohibits anyone pretending to be you from opening a new account.
- Guard your Social Security Number. Don't carry your card with you! Secure paperwork that includes your SSN.
- Ignore calls or emails asking for your personal information. You should initiate any communication that requires it.
- Don't open email attachments from unknown sources.
- Consider using a credit and identity theft monitoring service.
- Use strong passwords. Also, avoid obvious security questions (it's not hard to find your pet's name, city where you were born, or maiden name on social media.)
- Monitor your bank statements and credit card reports regularly.
- Hold your mail when leaving town.
- Shred statements containing personal information before trashing them, especially junk mail offering pre-approved credit offers. (Yes, people troll the garbage.)
- Add security software to your PC, laptop, tablet.
- Avoid connecting to public WiFi (i.e. airport, coffee shops) if possible.
- Consider a digital wallet. It's an app with digital, encrypted versions of your credit and debit cards. Bonus: it's contactless, so fewer health risks.
- Lock your mobile devices with a code or password. (Consumer Reports says only 36% of American smartphone users set a pin to lock their phones.)

[1] https://bwnews.pr/3ri3xeB