Androscoggin Bank Top 10

COVID Scams Survival Guide

We've posted a few articles about the rise of scams during the era of COVID-19. It is unfortunate that during such dynamic times, there are those who would seek to capitalize on the fear and misfortune of others. These are 10 Tips to keep you and those you care about safe from COVID-19 Scams.

1

Watch out for phishing scams.

Phishing scams use fraudulent emails, texts, phone calls and websites to trick users into disclosing private account or login information. Do not click on links or open any attachments or pop-up screens from sources you are not familiar with; if something seems suspicious then it probably is. Best practice is to go the website directly rather than through a link if you think there is any chance of it being malicious. Make sure you **NEVER** give your password, account number or PIN to anyone.

2

Ignore offers for a COVID-19 vaccine, cure or treatment.

If there is a medical breakthrough, it will be in the news and public sphere. A miracle cure will not come through unsolicited emails or online ads.

3

Rely on official sources for the most up-to-date information on COVID-19.

We've already compiled a list of trusted sources from the Centers for Disease Control to the Federal Deposit Insurance Corporation to the Department of Homeland Security. To view the best places to stay updated with the trusted information CLICK HERE.

4

Remember that the safest place for your money is in the bank.

It's physically secure and it's federally insured. When you deposit your money at a bank, you get the comfort of knowing that your funds are secure and insured by the government.

5

Research any organization before giving a donation.

Be wary of any business, charity or individual requesting COVID-19-related payments. A red flag is if they ask for donations in cash, by wire transfer, gift card or through the mail.

6

Keep your computers and mobile devices securely up to date.

Using the latest security software, web browser, and operating system is the best defenses against viruses, malware and other online threats. Turn on automatic updates so you receive the newest fixes as they become available.

7

Recognize and avoid fake website links.

Cybercriminals embed malicious links to download malware onto devices or route users to bogus websites. Hover over suspicious links to view the actual URL where you will be routed. Fraudulent links are often disguised by simple changes in the URL. For example: ABC-Bank.com vs ABC_Bank.com.

8

Change your security settings to enable multi-factor authentication for accounts that support it.

Multi-factor authentication—or MFA—is a second step to verify who you are, such as a text with a code. This may seem like a hassle to get into your accounts or login into a website you frequently use, but it is a strong defense against bad actors seeking to capture your information.

9

Before you make any investments, remember the high potential for fraud right now.

You should be wary of any company claiming the ability to prevent, detect or cure coronavirus. For information on how to avoid investment fraud, visit the U.S. Securities and Exchange Commission website.

10

Report any coronavirus scam(s) you see.

Visit the FBI's Internet Crime Complaint Center at www.ic3.gov to report suspected or confirmed scams. You can also stay up-to-date on the latest scams by visiting the FTC's coronavirus page.