Bluff View Bank
Focused On You

Our security training vendor, KnowBe4 has the following helpful tips for protecting your money, identity and confidential information during the COVID-19 crisis:

Working from Home? Don't Fall for This "Phony" Call

The Coronavirus Disease 2019 (COVID-19) pandemic has caused a massive shift in the number of employees who are working remotely. From a cybercriminal's perspective, this is a perfect opportunity for their social engineering scams.

One scam involves cybercriminals calling you and posing as support personnel from the companies or services that your organization may be using to allow you to work remotely. Typically, the caller will try to gain your trust by stating your job title, email address, and any other information that they may have found online (or on your LinkedIn profile). Then, the caller claims that they will send you an email that includes a link that you need to click for important information. Don't fall for this scam!

Remember the following to help protect yourself from these types of scams:

- Never provide your personal information or work information over the phone unless you're the one who initiated the call.
- Scammers can spoof any number they'd like. Therefore, even if a call looks like it's coming from a legitimate source, it could be a scam.
- If you receive this type of call, hang up the phone immediately and notify the appropriate team in your organization.

Watch Out for New COVID-19 Data

With thousands of new cases of Coronavirus (COVID-19) being recorded daily, the bad guys know that people are afraid and they plan to exploit that fear. They are sending phishing emails claiming to have official "new" or "updated" data on Coronavirus in your area. These emails are intense, urgent, and are designed to spark a knee-jerk reaction. Don't fall victim to their scare tactics!

Remember the following to protect yourself:

- Think before you click. The scammers are expecting an impulsive click.
- Never click a link or attachment from an email you weren't expecting.
- Stay informed by going directly to a trusted news source for information about Coronavirus such as the Center for Disease Control (CDC) or the World Health Organization (WHO).

Beware of Fake COVID-19 Stimulus Packages

Cybercriminals are willing to exploit every aspect of the Coronavirus crisis. The recent plan of a US Stimulus package is just one more thing they can use to their advantage. Watch out for phony emails promising information on how the stimulus package will benefit you. They could appear to be from the IRS, government officials, or even your HR Department. Some of these fake emails may even offer access to the money right away. Don't fall for it!

Here's some tips to help you stay vigilant:

- Remember that if something seems too good to be true, it probably is.
- When questioning the legitimacy of an email sent from an organization or company, give them a call! One quick call could save you or your organization from a potential data breach.

Stimulus payments will come from the Internal Revenue Service (IRS). The IRS will not contact you via email without your consent. If you receive an email from the IRS, we recommend visiting the official website and logging in directly.

Watch Out for Fake Charities

With the Coronavirus pandemic still raging on, people all over the world are doing what they can to help one another. The bad guys are hoping to use this compassion to their advantage. They are posing as charitable organizations that claim to fund research, support hospitals, or provide help to victims of the virus. Don't be fooled!

Want to donate to *real* causes? Here are some tips:

- **Do your research.** Use a trusted website like Charity Navigator to research an organization before making donations.
- **Reach out.** Contact your charitable organization of choice directly by going to their website or calling your local chapter.

Never trust a link. Even if the email appears to be sent from a legitimate organization, type the webpage into your browser instead of clicking a link provided in an email.

Additional Scams Targeting Seniors

- **Medical Provider scams.** Fraudsters pretending to be doctors or other hospital staff are claiming to have treated relatives or friends of the intended victim for COVID-19 and are demanding payment for treatment.
- **Bank & FDIC scams.** Scammers impersonate FDIC or bank employees and falsely claim that banks are limiting access to deposits or that there are security issues with bank deposits.
- **Investment scams often styled as "research reports."** Fraudsters claim that products or services of publicly traded companies can prevent, detect or cure COVID-19.

Stop, Look, and Think. Don't be fooled.
KnowBe4.com