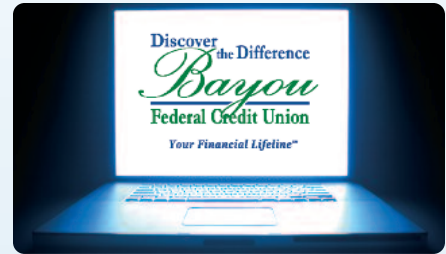


Coronavirus

Cyber Security Update 1

March 12, 2020



The emergence of the Coronavirus has brought about fears and concerns for people across the globe. Now scammers are taking the opportunity to trick people into giving out personal information. Bayou Federal Credit Union is monitoring the situation and urges you to be on the lookout for scams, fake e-mails, texts, and social media posts related to this event.

Beware of fake e-mails, texts, and social media posts related to Coronavirus!

According to the Federal Trade Commission (FTC) and the World Health Organization (WHO), scammers are setting up websites to sell bogus products, and using fake e-mails, texts, and social media posts as a ruse to take your money and get your personal information.

The e-mails and posts may be promoting awareness and prevention tips, and even fake information about cases in your area. They also may be asking you to donate to victims, offering advice on unproven treatments, or contain malicious e-mail attachments.

Bayou Federal Credit Union urges you to be cautious, and on the lookout for scams and malicious messages. Here are some tips to help you keep the scammers at bay:

- Don't click on links from sources you don't know. It could download a virus onto your device.
- Make sure the anti-malware and anti-virus software on your computer is up to date.
- Watch for emails claiming to be from the Centers for Disease Control and Prevention (CDC) or experts saying that have information about the virus. For the most up-to-date information about the Coronavirus, visit the Centers for Disease Control and Prevention (CDC) and the World Health Organization (WHO).
- Ignore online offers for vaccinations.
- If you see ads touting prevention, treatment, or cure claims for the Coronavirus, ask yourself: if there's been a medical breakthrough, would you be hearing about it for the first time through an ad or sales pitch?
- Do your homework when it comes to donations, whether through charities or crowdfunding sites. Don't let anyone rush you into making a donation. If someone wants donations in cash, by gift card, or by wiring money, don't do it.
- Be alert to "investment opportunities." The U.S. Securities and Exchange Commission (SEC) is warning people about online promotions, including on social media, claiming that the products or services of publicly-traded companies can prevent, detect, or cure coronavirus and that the stock of these companies will dramatically increase in value as a result.

For more information, visit the official websites of the FTC and WHO. Here are their web addresses:

Federal Trade Commission - www.consumer.ftc.gov

World Health Organization - www.who.int

To report a scam or ID Theft:

If you believe you are the victim of identity theft, you should contact the proper law enforcement authorities, including local law enforcement, and you should consider contacting your state attorney general and/or the Federal Trade Commission ("FTC").

You also may contact the FTC to obtain additional information about avoiding identity theft.

Federal Trade Commission, Consumer Response Center

600 Pennsylvania Avenue NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338) www.ftc.gov/idtheft