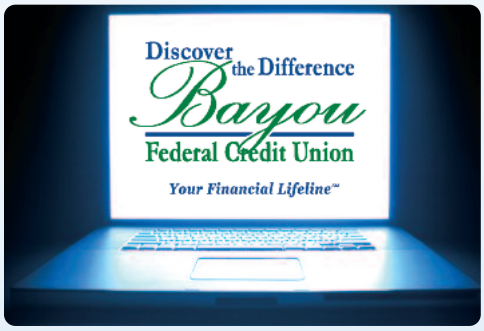
Coronavirus

Cyber Security Update 2

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.

The World Health Organization (WHO) posted this information in February, 2020:

Beware of criminals pretending to be WHO

Criminals are disguising themselves as WHO to steal money or sensitive information. If you are contacted by a person or organization that appears to be from WHO, verify their authenticity before responding.

The World Health Organization will:

- **never ask you to login to view safety information**
- **never email attachments you didn't ask for**
- **never ask you to visit a link outside of www.who.int**
- **never charge money to apply for a job, register for a conference, or reserve a hotel**
- **never conduct lotteries or offer prizes, grants, certificates or funding through email**
- **never ask you to donate directly to emergency response plans or funding appeals.**
- **Beware that criminals use email, websites, phone calls, text messages, and even fax messages for their scams.**

You can verify if communication is legit by contacting WHO directly.

Phishing: malicious emails appearing to be from WHO

WHO is aware of suspicious email messages attempting to take advantage of the 2019 novel coronavirus emergency. This fraudulent action is called phishing.

These "Phishing" emails appear to be from WHO, and will ask you to:

- give sensitive information, such as usernames or passwords
- click a malicious link
- open a malicious attachment.

Using this method, criminals can install malware or steal sensitive information.

How to prevent phishing:

- Verify the sender by checking their email address.

- Make sure the sender has an email address such as 'person@who.int' If there is anything other than 'who.int' after the '@' symbol, this sender is not from WHO. (WHO does not send email from addresses ending in '@who.com' , '@who.org' or '@who-safety.org' for example.)

- Check the link before you click. Make sure the link starts with 'https://www.who.int'. Better still, navigate to the WHO website directly, by typing 'https://www.who.int' into your browser.

- Be careful when providing personal information. Always consider why someone wants your information and if it is appropriate. There is no reason someone would need your username & password to access public information.

see page 2 ...

continued from page 1 ...

• Do not rush or feel under pressure. Cybercriminals use emergencies such as 2019-nCov to get people to make decisions quickly. Always take time to think about a request for your personal information, and whether the request is appropriate.

• If you gave sensitive information, don't panic. If you believe you have given data such as your username or passwords to cybercriminals, immediately change your credentials on each site where you have used them.

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

Bayou Federal Credit Union 3-2020