Western Alliance Bank®

CYBER SECURITY

COVID-19 PHISHING ALERT

WHAT IS "PHISHING"?

Phishing is a type of cybercrime that uses emails disguised as coming from a person or organization you trust, in order to lure you into clicking a fraudulent link or providing access to sensitive information.

WHY ARE YOU AT RISK?

Hackers are actively targeting your organization because you have information that is valuable to them. They may be after your customer, patient, student, or employee data. They could also be interested in your intellectual property, financial account information, or payment card data. If one employee falls for a phishing attack, your entire system may be at risk.

WHAT YOU SHOULD DO IF YOU GET A SUSPICIOUS EMAIL:

If you suspect that an email is a phishing email:

- Do not open any links or attachments in the email
- Notify your IT or Information Security department immediately

In the wake of COVID-19, fraudulent cyber and email schemes are on the rise. Be aware of emails that impersonate a reliable source like the Center for Disease Control and Prevention (CDC) or the World Health Organization (WHO), or look to be from legitimate sources with information on COVID-19 compensation, insurance, or donation topics. These phishing emails steal credentials, infect systems with ransomware, or commit fraud.

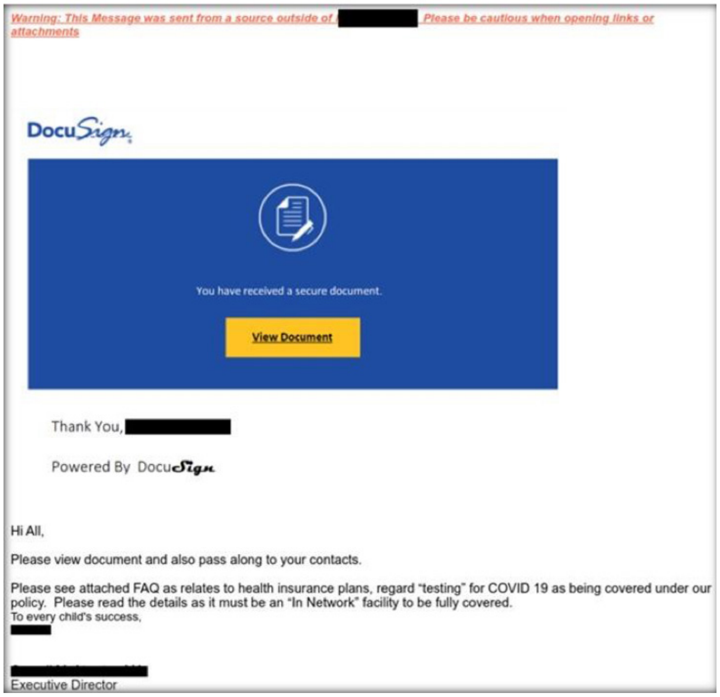
TIPS TO IDENTIFY A PHISHING EMAIL

- The email includes a request for your username and/or password, either by replying to the email or by clicking a link that takes you to a site where you're asked to input your information.
- The email includes links or email addresses that, when you hover over them, list a different destination than described.
- You don't know the sender, and the email has an unexpected attachment.
- There are grammatical errors in the email or subject line.
- The email contains email addresses that don't match between the header and the body, are misspelled (**like @gmaill.com**) or have unusual formats (**@company-othersite.com**).
- There is a sense of urgency to try to get you to respond.

See below for examples of real phishing emails that scammers have sent impersonating real organizations in attempts to steal credentials, spread ransomware and commit fraud.

EXAMPLE 1

This phishing email uses a fake secure DocuSign notification, claiming to provide FAQs as they relate to a health insurance plan and COVID-19 coverage. This phish can steal credentials or spread ransomware.



Warning: This Message was sent from a source outside of [redacted] *Please be cautious when opening links or attachments*

You have received a secure document.

Thank You, [redacted]

Powered By DocuSign

Hi All,

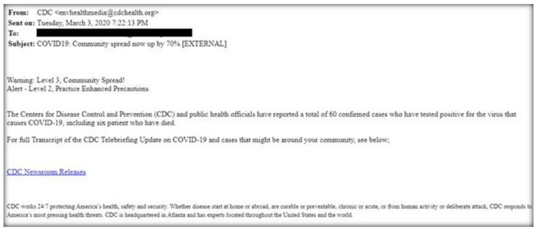
Please view document and also pass along to your contacts.

Please see attached FAQ as relates to health insurance plans, regard "testing" for COVID 19 as being covered under our policy. Please read the details as it must be an "In Network" facility to be fully covered.
To every child's success,
[redacted]

[redacted]
Executive Director

EXAMPLE 2

The threat actor registered a fake CDC domain to lure the recipient into clicking on a link and spreading ransomware.



From: CDC <envhealthmedia@cdchealth.org>
Sent on: Tuesday, March 3, 2020 7:22:13 PM
To: [redacted]
Subject: COVID19: Community spread now up by 70% [EXTERNAL]

Warning: Level 3, Community Spread!
Alert - Level 2, Practice Enhanced Precautions

The Centers for Disease Control and Prevention (CDC) and public health officials have reported a total of 60 confirmed cases who have tested positive for the virus that causes COVID-19, including six patient who have died.

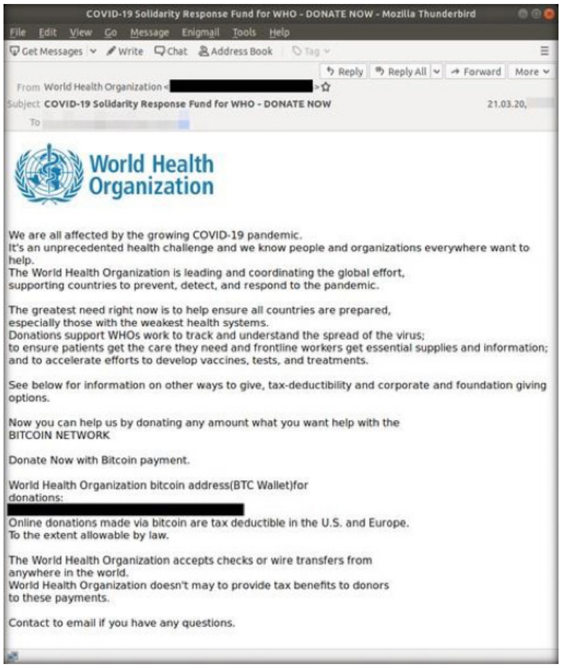
For full Transcript of the CDC Telebriefing Update on COVID-19 and cases that might be around your community, see below;

CDC Newsroom Releases

CDC works 24/7 protecting America's health, safety and security. Whether disease start at home or abroad, are curable or preventable, chronic or acute, or from human activity or deliberate attack, CDC responds to America's most pressing health threats. CDC is headquartered in Atlanta and has experts located throughout the United States and the world.

EXAMPLE 3

This phishing email uses a WHO spoofed email address in a donation scam. In it, the cybercriminal is asking for cryptocurrency transfer via Bitcoin wallet. If executed, there is little chance the transaction could be reversed.


COVID-19 Solidarity Response Fund for WHO - DONATE NOW - Mozilla Thunderbird
File Edit View Go Message Enigmail Tools Help
Get Messages
Write
Chat
Address Book
Tag
Reply
Reply All
Forward
More
World Health Organization

From World Health Organization <[redacted]>
Subject **COVID-19 Solidarity Response Fund for WHO - DONATE NOW** 21.03.20,
To

We are all affected by the growing COVID-19 pandemic.
It's an unprecedented health challenge and we know people and organizations everywhere want to help.
The World Health Organization is leading and coordinating the global effort,
supporting countries to prevent, detect, and respond to the pandemic.

The greatest need right now is to help ensure all countries are prepared,
especially those with the weakest health systems.
Donations support WHOs work to track and understand the spread of the virus;
to ensure patients get the care they need and frontline workers get essential supplies and information;
and to accelerate efforts to develop vaccines, tests, and treatments.

See below for information on other ways to give, tax-deductibility and corporate and foundation giving options.

Now you can help us by donating any amount what you want help with the
BITCOIN NETWORK

Donate Now with Bitcoin payment.

World Health Organization bitcoin address(BTC Wallet)for
donations:
[redacted]
Online donations made via bitcoin are tax deductible in the U.S. and Europe.
To the extent allowable by law.

The World Health Organization accepts checks or wire transfers from
anywhere in the world.
World Health Organization doesn't may to provide tax benefits to donors
to these payments.

Contact to email if you have any questions.

Legitimate information about the Coronavirus from the Centers for Disease Control and Prevention (CDC) and World Health Organization (WHO) on the Coronavirus can be found on their websites listed below.

(CDC) https://www.cdc.gov/coronavirus/2019-ncov/index.html

(WHO) https://www.who.int/health-topics/coronavirus

Forbes 2020
BEST BANKS
IN AMERICA

Western Alliance Bancorporation has ranked in the top 10 on the *Forbes* Best Banks in America list for five consecutive years, 2016-2020.

westernalliancebank.com | (800) 764-7619

Alliance Bank of Arizona | Bank of Nevada | BridgeBank
First Independent Bank | Torrey Pines Bank | Alliance Association Bank

Divisions of Western Alliance Bank. Member FDIC.