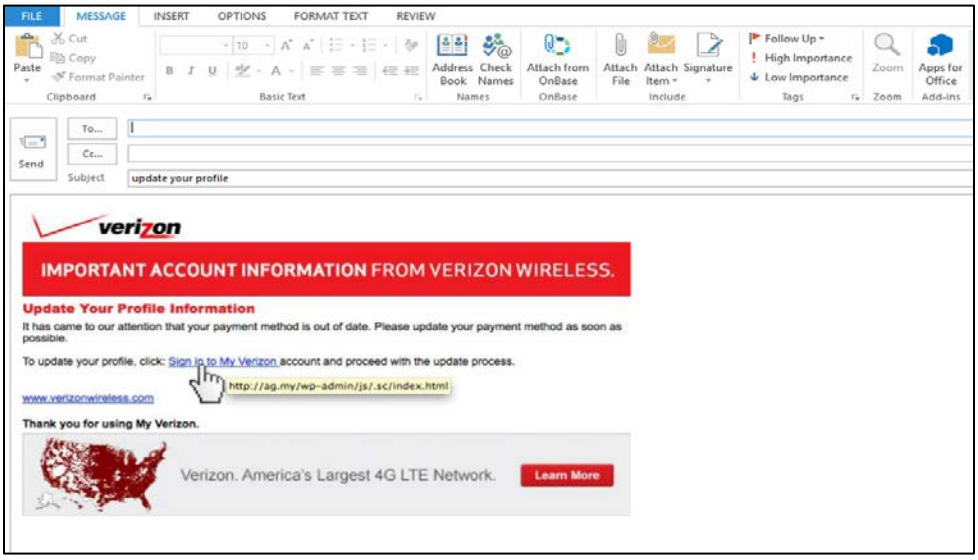
Catholic Mutual…"CARES"

Cyber/Phishing Scams During the COVID-19 Crisis

Cyber criminals are using the COVID-19 crisis as an opportunity to take advantage of people by requesting personal information or asking for donations to fraudulent charities/causes. Individuals must be aware of increased exposure to email and phone scams due to the COVID-19 pandemic. It is imperative to exercise caution in handling any email with a COVID-19-related subject line, attachment or hyperlink. In addition, you should be guarded when it comes to text messages and/or phone calls related to COVID-19.

Catholic Mutual Group encourages taking the following precautions:

- Ensure updated incident response plans are in place and consider changes in the work environment, such as employees working remotely and using mobile devices for business purposes. Increased awareness for information technology security is critical.
- Use suspicion when screening emails and phone calls related to COVID-19.
- Do not respond to unsolicited requests for personal information, whether by email, phone or text message. If someone requests personal information through an email or call, immediately delete the email or end the call. Do not provide personal information unless you can verify the identity/authority of the source requesting information. If you think the request is valid but can't verify the identity of the requester, call the organization yourself to know for sure who you are talking with.
- Avoid clicking on links in unsolicited emails and be wary of email attachments. Before clicking on any links in an email, hover your mouse over the link and the actual URL will appear. Please ensure the URL is linked to the right address. Hackers often spoof the URL to look like a legitimate address. This scam is often applied by phishers utilizing companies which are reliable, well-known, and likely to have large user consumer base clients (i.e., banks, credit card company, online shopping company, and even your wireless phone carrier as illustrated below)



- If you happen to receive an email that seems suspicious, do not copy and paste any link into a search browser, forward the suspicious email to others, or solely rely on anti-virus software to catch it. These decisions could result in a cyber-criminal gaining access to your network putting personal and confidential information at risk.
- When searching for education and guidance on COVID-19, only use trusted/legitimate sources, such as government websites like the CDC and your State/Local Health Departments for acquiring up-to-date and fact-based information.
- You may be solicited by companies or individuals with respect to any COVID-19 related transactions (i.e., charitable donations, cleaning etc.) They may even offer to donate funds to you and ask for your bank account information. NEVER give out this information. Even a well-known source that appears to be legitimate could, in fact, be fraudulent. A best practice to better protect you from scams is for you to seek out your own needs rather than accepting solicitation from sources with potential scams.

If a cyber incident does occur at your organization, immediately notify your IT personnel. To report a claim during business hours, please contact Jeff Schneider, Director of Claims at Catholic Mutual Group, at 800-228-6108 ext. 2404 (office) or 402-490-0021 (mobile). During non-business hours, please contact our cyber insurance experts, Tokio Marine HCC, at 1-888-627-8995 and be sure to identify yourself as a Catholic Mutual Member.

Should you need any further assistance during this time, please do not hesitate to contact your Risk Management Representative.

In addition to the aforementioned cyber/phishing scams, please be aware of other fraudulent activities that are occurring. If you are a facility which requires the use of the N-95 masks, be aware of fraudulent products currently being circulated. See below link for example:

https://www.cdc.gov/niosh/npptl/usernotices/counterfeitResp.html

(Revised 05/2020)