

Tower Federal Credit Union

COVID-19 Security Awareness

In this time of global uncertainty, there are those who try to prosper from illegal activities. Tower wishes to remind you that cyber attackers do not take breaks, and instead focus on these media-intense events by preying on individual's fears. Scams and phishing attacks to install malware, gain control of your system, or trick you to donating money to fraudulent charities or causes are becoming more common, and can happen at work or at home, via email, text messages, or even via phone call. Please exercise caution in handling any communication relating to COVID-19, including social media pleas, texts, calls, email attachments, or web hyperlinks.

Below are some common indicators that you may be viewing a scam or phishing attack:

- Messages that communicate a **sense of urgency**. Attacks thrive on making you rush before thinking about what you're actually doing.
- Messages that pressure you into **bypassing** or **ignoring** security policies and procedures.
- Messages that promote **miracle cures**, such as vaccines or medicine that will protect you from COVID-19. If it sounds too good to be true, it most likely is.
- Phone calls or messages that **pretend** to be an official or government organization, often urging you to take immediate action.
- **Verify** not only the sender of an email, but any hyperlinks that may be included within the email, before clicking on them.

The following are tips from the [Federal Trade Commission](#) (FTC) to help you avoid COVID-19 scammers:

- Don't click on links from sources you don't know. They could download viruses onto your computer or device.
- Watch for emails claiming to be from the Centers for Disease Control and Prevention (CDC) or experts saying they have information about the virus.
- Ignore online offers for vaccinations. There currently are no vaccines, pills, potions, lotions, lozenges or other prescription or over-the-counter products available to treat or cure Coronavirus disease 2019 (COVID-19) — online or in stores.
- 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.

The [Cyber and Infrastructure Security Agency](#) (CISA) also has advice on combating cyber threats:

- Avoid clicking on links in unsolicited emails and be wary of email attachments.
- Use trusted sources—such as legitimate, [government websites](#)—for up-to-date, fact-based information about COVID-19.
- Do not reveal personal or financial information in email, and do not respond to email solicitations for this information.
- Verify a charity's authenticity before making donations. Review the Federal Trade Commission's page on [Charity Scams](#) for more information.



Information Security and
Technology

Tower Federal Credit Union COVID-19 Security Awareness

Below are some, but not all, examples of potential scams and phishing attempts relating to COVID-19:

Fake Insurance Email:

Insurance coverage update reminder

Thank you for ordering Coronavirus (COVID-19) insurance cover from Cigna.

Please remember to locate your latest payment report in the link under

**Here's your Payment invoice
#1731**

Do not think twice to make contact with us. We are always happy to help you.
You can find all our contact details and huge selection of info on your individual web page or perhaps the mobile app.

Please note: This specific e mail along with it's content are confidential and meant solely for the addressee. Kindly alert the message sender in case you have received this letter by mistake or just delete it

© 2020 Cigna. All rights reserved

[Unsubscribe](#) [ABOUT US](#) | [TERMS AND CONDITIONS](#) | [HELP](#)

Fake email request for more information:

Corona Virus - Do this before it's too late...

- ① This message was moved to the Junk Email folder because you only trust email from senders in your Safe Senders list. It's not junk | [Show blocked content](#)
- ① This message was sent with High importance.
- ① Flag for follow up.

 Pandemic Survival <hoK12•@touring.wandtype.com>
Fri 13/03/2020 11:01



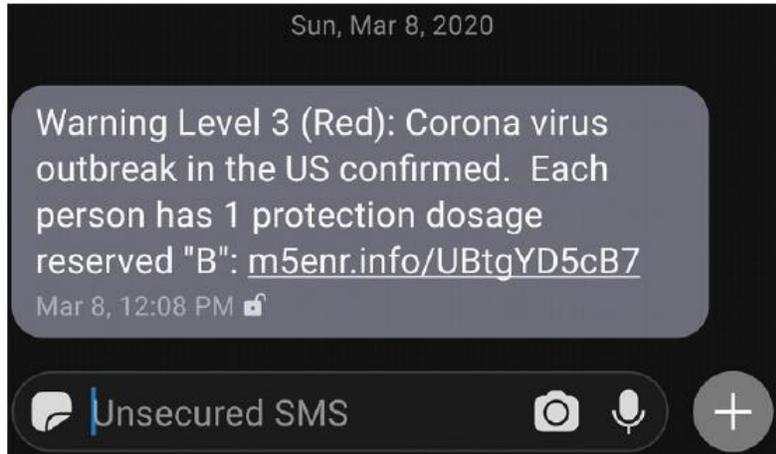
[Corona Virus - Do this before it's too late...](#)



Information Security and
Technology

Tower Federal Credit Union COVID-19 Security Awareness

Fake SMS message:



Fake Social Media Message

All employees will receive (mandatory) paid leave to avoid the spread of the COVID-19 novel coronavirus starting from March 13, 2020. Offices will resume after 2 weeks of the mandatory closure. Check the link to see if your company is listed: <http://bit.ly/MandatoryPaidLeave> 17:43

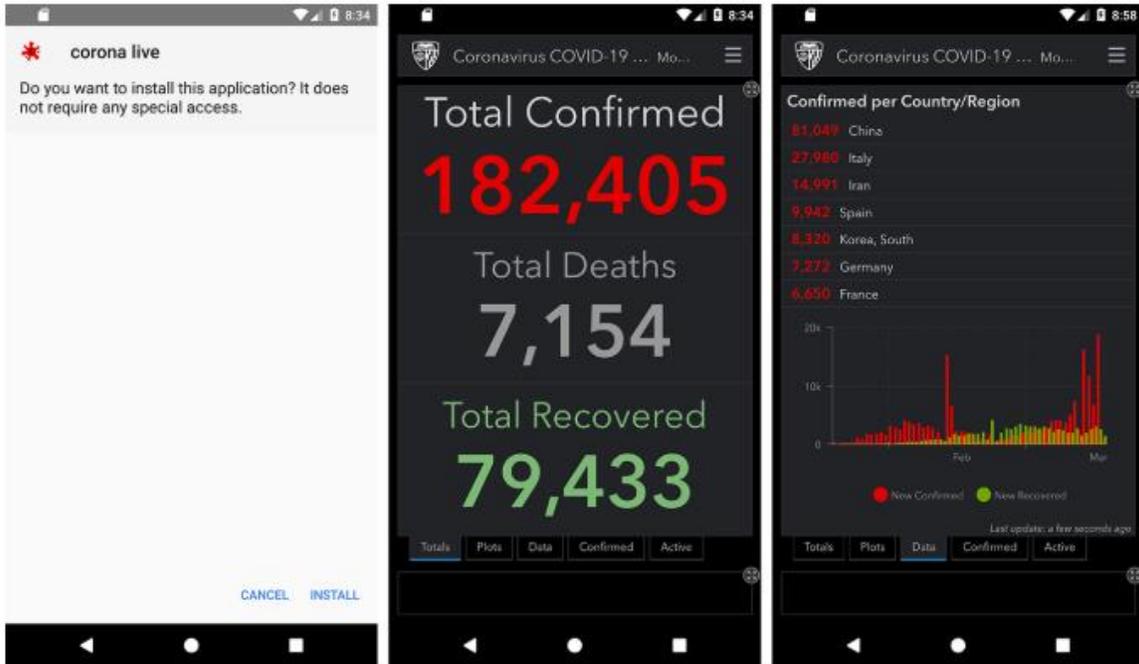


Information Security and
Technology

Tower Federal Credit Union

COVID-19 Security Awareness

Fake mobile application map of COVID-19 cases:



Screenshot of the application when opened, and after a user allows the requested permissions to use the application.