Tower Federal Credit Union Information Security and Technology	**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** of 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.

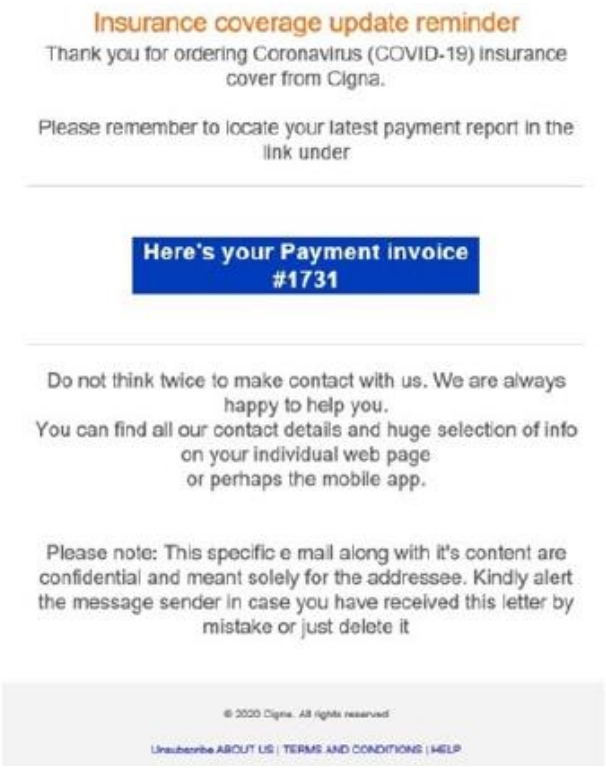
The Cyber and Infrastructure Security Agency (CISA) also has advice on combating cyber threats:

- 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.

Tower Federal Credit Union 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:

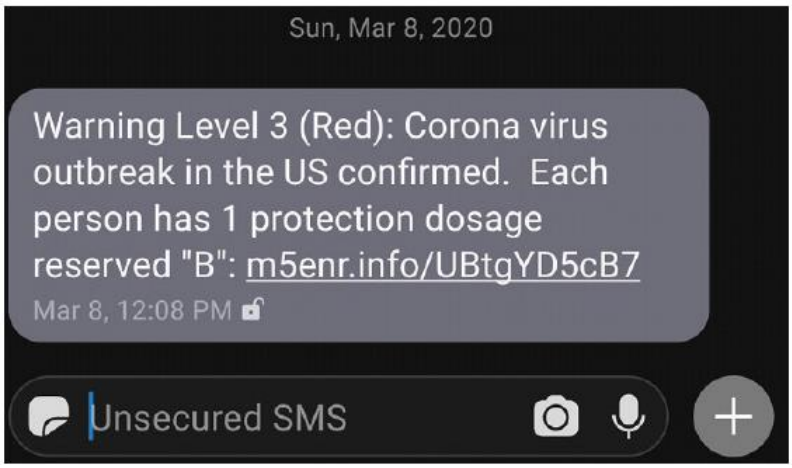
Fake Insurance Email:

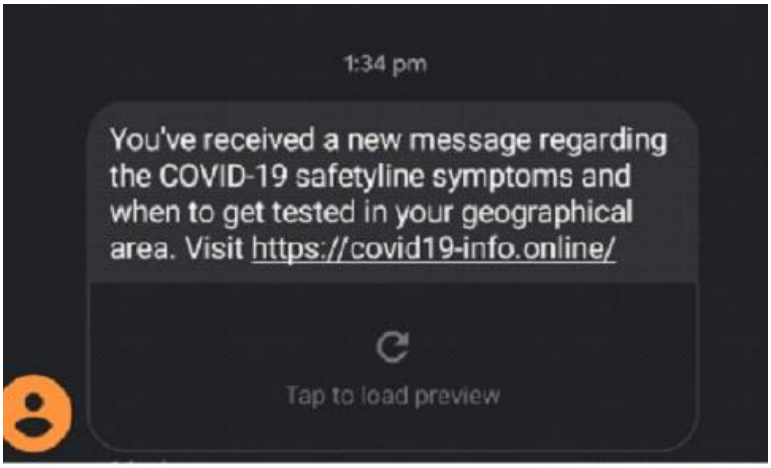


Fake email request for more information:

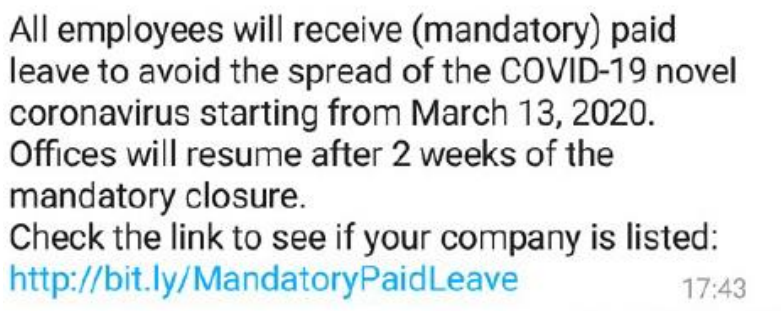
Tower Federal Credit Union Information Security and Technology	**Tower Federal Credit Union** **COVID-19 Security Awareness**

Fake SMS message:



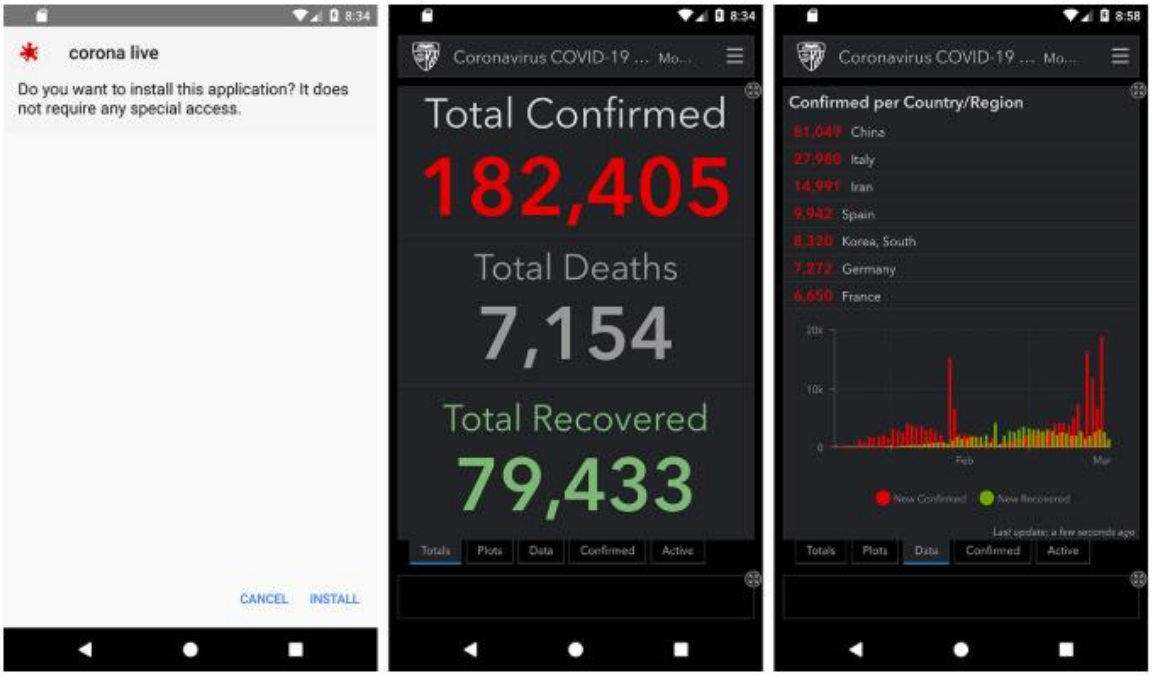


Fake Social Media Message



Tower Federal Credit Union 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.