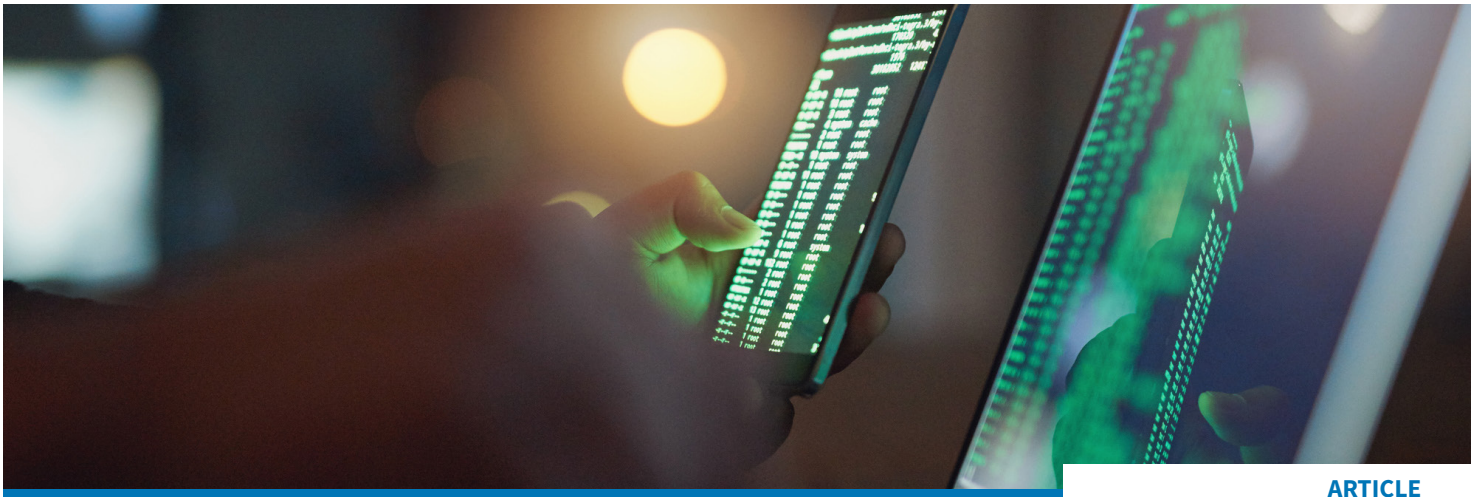

ARTICLE

How can you prevent fraud in the COVID-19 era?

With the onset of a new normal for most businesses due to the spread of COVID-19, fraudsters have found new ways to continue their business. End-users are often the weak links exploited by these fraudsters to carry out their operations, impacting not only the users themselves, but also the organisation. Below, FTI Consulting highlights some of the most prevalent types of fraud.

Types of frauds and their intent

Donation requests:

Fraudsters may attempt to steal your credentials or funds, by sending fraudulent links or posing as charitable organisations.

Account takeover/ account breach:

Fraudsters can attempt to takeover your accounts (eWallet/ bank account/ shopping app wallets) by claiming that the account has been deactivated/ suspended.

COVID-19 related information:

Unauthorised apps and websites claiming to provide health tests/ symptom checking/tracking services could be used to steal your personal and financial data.

Phishing attack:

Fraudsters are known to send emails posing as personal acquaintances or charitable organisations, asking for financial help.

Online apps/ networks:

With many people turning to social connectivity apps, fraudsters can use this opportunity to steal your data, cause financial loss or invade your privacy.

Links, images and documents shared on social networks could be misused as malware vehicles.

Hacking remote networking and co-working apps:

There have been cases of uninvited attendees accessing meetings to listen in or access data.

eCommerce:

Sale of scarce items from unknown sellers/ websites often serve as honeypots for data theft and financial fraud.

Notices of fines due to breach of lockdown:

Fraudsters could spoof the actions taken by authorities, to extort unsuspecting targets.

Scenario	Intent	Do's	Don'ts
Donation requests: — You may receive messages/ emails asking for donations and contributions to known or new organisations, to help in these tough times. — The sender could be known or unknown to you.	 Financial Fraud	✓ Check the credentials of the charity/ organisation through independent research. ✓ Visit the organisation's website by searching in google to validate the existence of the cause/ donation. ✓ Pay through the official website.	X Click on the link provided in the message/ email. X Call the number provided in the message. X Forward the message without checking the authenticity.
Account takeover/ breach attempt: — You may get a message/ email from your service provider (bank/ ewallet company/ app wallets), stating that the account had been frozen or suspended. To unlock and regain access, click on this link or call on this number. — As Indian banks have been asked to allow customers to postpone their loan EMIs, Indian customers may get calls/messages, asking them to share OTP to activate the postponement.	 Financial Fraud	✓ Check the details of the sender, look for spelling mistakes, check if the sender name is related to the supposed sender (if the message is supposed to be from PayTM, is the sender name appearing as TmPay?). ✓ If you have an account, login to confirm if the lock-out / postponement offer is real. ✓ Visit the service provider's website to get the correct contact details.	X Call the number given in the message or click on the link provided. X Provide any confidential details of the account (password/ OTP/ CVV number/ card expiry) to anyone. X Use the number appearing in Google search results to contact the service provider.
COVID-19 related links: — You may receive links to apps or webpages offering details of COVID-19. These could relate to tracking the spread in your city, country or the world. Alternatively, the app could be a supposed symptom checker. — The message may have come from known or unknown persons.	 Data Theft	✓ Be wary of unsolicited links. ✓ Visit the links only if you trust the websites.	X Download the apps without checking the rating, count of downloads or date of release. X Open links leading to lesser known/ unknown websites. X Download any files or add-ons, or grant permissions on your device.
Phishing attack: — You may receive an email/ SMS/WhatsApp message from someone you know, asking for help. — This message may ask you to click on the given links to take action (money or enter login credentials).	 Data theft/ financial fraud	✓ Reach out to the person separately to confirm the authenticity of the request. ✓ If unable to get through, do not take any action on the message. ✓ Review the details of the sender closely for differences in spelling and contact numbers.	X Reply to the email/ message or click on the link or download attached files. X Share any confidential information (bank account details/ login credentials/OTP).

Scenario	Intent	Do's	Don'ts
Online apps/ networks: — You may receive links for new apps/ websites from known or unknown persons. — These apps could be for games/ social connectivity/ online learning.	 Data theft/ financial fraud	✓ Reach out to the person separately to confirm the authenticity of the invitation. ✓ Ensure that the sender has used the app and is not just forwarding the message received on another group. ✓ Check the rating, reviews, count of downloads, date of release for yourself before taking any action.	X Forward similar links received from others without authenticating the security of the app. X Download any files or add-ons, or grant permissions on your device.
Hacking remote networking and co-working apps: — You may notice some attendees in your meeting that are unknown or not invited. — You may receive an unexpected invite for a meeting from a known or unknown sender.	 Data Theft	✓ Require passwords for attendees to join meetings. ✓ Enable the 'waiting room' feature, allowing the host to see the attendees before they join the meeting. ✓ Once all expected participants have joined, lock the meeting.	X Join meetings or click on links without confirming authenticity with the sender. X Share the meetings invite links on social media/ public platforms. X Discuss or share sensitive or confidential content. X Post photos of your meetings online.
Links, images and documents being shared on social networks and IMs: — You may receive links, images, videos, documents over social media and IMs from known or unknown persons.	 Spread malware	✓ Deactivate automatic download of media files on your apps. ✓ Request your group members/ connections to only share verified, authenticated, relevant and important content. ✓ Be judicious in downloading/ viewing/ sharing content shared with you.	X Blindly forward content received from others, without checking its authenticity.
Offer of sale of scarce items, from unknown sellers/ websites: — Considering the scarcity of items, some sellers may be offering to sell/ deliver the items. — The message may be accompanied by a phone number/ web address/ link.	 Data theft/ financial fraud	✓ Adhere to the regulations/ guidelines shared by your local government regarding deliveries and essential services.	X Reach out to the supposed seller on any of the mediums suggested. X Share your details such as bank/ card details.
Notices of fines due to breach of lockdown: — Some entities may pretend to be government representatives and demand the payment of fines for breaching the lock-down/ government guidelines. — This attempt is likely to be done remotely i.e. over email/ message/ phone.	 Extortion	✓ Ask for details of the breach incident i.e. when and where were you observed to be violating the guidelines and how did they find you in order to validate the authenticity of the claim.	X Don't share any confidential data like bank/ card details, login credentials or details of your movements.

The views expressed herein are those of the author(s) and not necessarily the views of FTI Consulting, Inc., its management, its subsidiaries, its affiliates, or its other professionals.

FTI Consulting, Inc., including its subsidiaries and affiliates, is a consulting firm and is not a certified public accounting firm or a law firm.

NUPUR LADHA
Senior Director
+91 99 3086 6259
nupur.ladha@fticonsulting.com

FTI Consulting is an independent global business advisory firm dedicated to helping organisations manage change, mitigate risk and resolve disputes: financial, legal, operational, political & regulatory, reputational and transactional. FTI Consulting professionals, located in all major business centres throughout the world, work closely with clients to anticipate, illuminate and overcome complex business challenges and opportunities.©2020 FTI Consulting, Inc. All rights reserved. **www.fticonsulting.com**