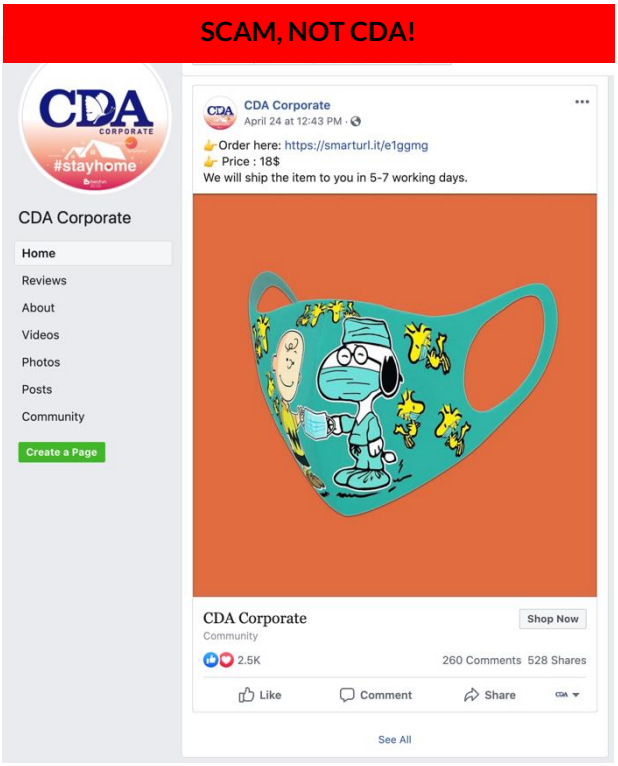
Helping You Avoid COVID-19 Online Scams

Dear Families and Providers,

I hope that you and your family remain in good health. As the novel Coronavirus (COVID-19) continues to impact the country, there has been an increase of scamming across the country. These scams are taking place both over the phone and online. Due to our increased screen time use for socialization, education, and entertainment during the stay-at-home order, we are seeing this outlet as one of the biggest means that scammers utilize to prey on users.

Important Notice: CDA has been informed of a scam!

Scammers often pose as well-known, trusted and authoritative sources. To the right is a screenshot of a Facebook Page falsely representing CDA to sell face masks. **CDA does not sell any product nor solicit request for payment of any kind. Please beware and do not send any payment or provide your personal information. If you have been a victim of this scam, please contact your local authorities.**



For the latest factual information about CDA and COVID-19, please visit our website www.cdasd.org/news.

CDA's Resource Team has gathered helpful information that can help protect you and your family from being victimized via phone call, email, or online (including ads and hyperlinks):

1. **A Feeling of Doubt or Distrust:** If it's coming from someone you don't know, can you verify if it is on behalf of an institution or an organization that you know well? For example, your bank. If so, the best thing to do is call them back directly to verify the information you are receiving or any requests for information.
2. **Directing me to "Click out":** Clicking on links, attachments, and ads can lead to phishing sites or immediate malware downloads. One way to see where a link may take you is to **hover your mouse over any hyperlinks**: Often, your email software should allow you to preview the URL associated with the hyperlink. Is the hyperlink a site that you recognize, or one that resembles another website but is purposely misspelled? If it resembles another website, you should flag the email as spam and delete it.
3. **A Sense of Urgency:** Scammers will often try to instill a sense of urgency, so that the victim doesn't have enough time to think things through. Watch out for timeframes that may seem like you need to "act fast."

Keep these tips in mind:

- Avoid opening any attachment or links in emails from senders that you don't recognize.
- Be careful of emails (or phone calls!) requesting account information or to verify an account. Businesses should never call you or email you directly to ask for your security credentials.
- Always verify that requests for information comes from a legitimate source. And when in doubt, put a website's domain into a browser yourself: Since most legitimate businesses use encryption known as Secure Socket Layer (SSL), "certificate errors" can be a warning sign that the website isn't valid.

Keeping Children Safe Online:

Children may be especially at risk for scams, since so much has shifted online. Distance learning, online chats with family, friends, and school is helpful in staying connected and encourages them to continue with their lives. However, it also presents many challenges. As parents and providers, it is highly recommended that you set time limits, use parental controls/privacy settings on devices, and/or have your children stay in open areas of the home. If you believe that you or someone in your family has been victimized by a COVID-19 scam, contact law enforcement immediately.

We hope that these tips and resources will help navigate through online scamming and protect you and your family during this time.

COVID-19 Resources on Scams

Click on the teal buttons below.

IRS-Tax Scams/Consumer Alerts:

https://www.irs.gov/newsroom/tax-scams-consumer-alerts
Learn more about identifying the signs of a scam.

Office of the Attorney General:

https://www.oag.ca.gov/charities
Learn more about charities scam.

FDA- US Food & Drug Administration:

https://www.fda.gov/news-events/press-announcements/coronavirus-covid-19-update-fda-alerts-consumers-about-unauthorized-fraudulent-covid-19-test-kits
FDA Alerts consumers about fraudulent Covid-19 test kits and more.

Federal Trade Commission:

https://www.consumer.ftc.gov/features/scam-alerts
Consumer information related to COVID-19 recent alerts and scams.

FBI-Public Service Announcement:

https://www.ic3.gov/media/2020/200401.aspx
Cyber-crime vulnerability tips.

Protecting Children, Victims and Survivors of Crime

Protecting Children Online:

https://www.sdcda.org/preventing/protecting-children-online/index.html
Learn effective ways to protect your children online.

San Diego District Attorney:

https://www.sdcda.org/Content/office/COVID%20Comprehensive%20Resources%20for%20Victims.pdf
Learn more about charities scam.

Additional Information

Internet Crimes Against Children Task Force at 1-800-843-5678.

CDA
Child Development Associates

For individualized assistance with resources or referrals during COVID-19 closure, please contact our Family Resources Team via email or by phone, during the hours of 8:30 a.m. to 5:00 p.m., Monday through Friday:

Jennifer Ordinario
Family Resources Supervisor
jordinario@cdasd.org
619-427-4411 x1416

Lidia Guzman
Family Resources Specialist
Bonita Office
lguzman@cdasd.org
619-427-4411 x1409

Alexandra "Alex" Real
Family Resources Specialist
Kearny Mesa Office
areal@cdasd.org
858-836-8065 x1775