Online scams increase during pandemic

The COVID-19 pandemic has led to a significant increase in dangerous and highly targeted online scams that take advantage of people’s fears and concerns. Users are tricked into clicking on links or attachments that contain computer malware. Education alone has seen a 660% increase in phishing emails using the virus to gain their victim's attention.

Here are some tips to avoid coronavirus phishing:

KEEP YOUR DEFENSES UP! Install, update and regularly run antivirus protection such as Symantec Endpoint Protection, available through the PCC Intraweb.

DON'T CLICK ON LINKS in text and emails from people and organizations you don't know. This goes for email on all subjects, not just COVID-19. Phishing by mobile text message is the fastest growing type online today.

DON'T GIVE OUT SENSITIVE OR PERSONAL DATA ONLINE especially from an unsolicited email or text messages. Caution with mobile chat apps like WhatsApp, Facebook Messenger, SnapChat and Telegram is also a smart move, especially with requests you don't recognize or expect.

LINK APPEARANCES IN MESSAGES CAN DECEIVE. The text of the link, and the site it links to are NOT ALWAYS THE SAME! Look-alike domain names are a go-to trick of these scamsters (cdc-com.com, instead of the real cdc.gov.)

When a message has been forwarded many times in a row, even if it arrives from a trusted sender, the contents may be misleading or contain dangerous links. Even friends and family can get caught in chain messages with questionable content.

Doctors and organizations like the WHO, CDC, NIH, and hospitals are OPEN INFORMATION SHARERS. Emails about 'secrets they don't want you to know,' brand-name drugs to avoid or that provide a cure or immunity, and mystery herbs/supplements are always worth your suspicion. At best they are unreliable medically, but links and attachments in them are certainly bad news.

REPORT, DON'T FORWARD! If something in your Inbox gives you doubt hit the report email button built into your G-mail screen. It's the stop sign with the exclamation point on it, and will make sure someone in security reviews it for you and the rest of the college. Forwarding suspicious emails to colleagues -- even in IT -- helps the crooks by spreading their dangerous content through the college.

If you're using VPN to work remotely, BE ESPECIALLY CAREFUL. A malware infection while VPN'd into the college can spread to other college equipment. If you wouldn't open it sitting at your desk, don't do it when working remotely.

You are our best line of defense against cyber-criminals preying on our collective fears and doubts. Thank you all for your continued vigilance as we defend Pima against this wave of pandemic-focused on-line crime.