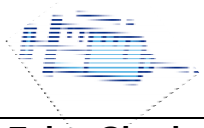
CYBERSECURITY EDUCATION

Rising Cyber Attacks amid the COVID-19 Outbreak

Coronavirus scams are spreading nearly as fast as the virus itself. As of July 26, 2020, the Federal Trade Commission (FTC) reported approximately 144,000 consumer complaints related to COVID-19 and stimulus payments. Below are some common scams to look out for.

Fake Government Announcements 	Threat actors are sending phishing emails disguised as government announcements. Fraudulent emails have included logos and other imagery associated with the Centers for Disease Control (CDC) and the World Health Organization (WHO). Emails include links to items of interest, such as "updated cases of the coronavirus near you," that lead to malicious sites designed to steal your email credentials.
Operational Disruption 	The spread of COVID-19 is disrupting temporary supplies and revenue in some industries. Emails disguised as invoices, shipping receipts, and job applications, include attachments that contain harmful malware or ransomware.
Hidden Malware 	There is a rise in malicious emails directing recipients to educational and health-related websites riddled with malware. A recent scam sends coronavirus maps loaded from legitimate sources that run malware in the background.
False Advice and Cures 	Emails purporting to hail from regional medical providers invite recipients to download attachments containing "secret cures" for the virus. The attachments instead contain malware designed to steal the personal and financial information of the victim.
False Charity 	Emails designed to mimic the CDC are soliciting donations to fight the spread of the virus. The emails appeal to recipients' altruism, urging victims to donate into a Bitcoin wallet or to make other types of payments. The CDC is a federal agency and does not solicit donations.

What can you do to protect yourself?

- Avoid online offers for coronavirus-related vaccines or cures.
- Be wary of emails, calls, and social media posts advertising "free" or government-ordered COVID-19 tests. Check the FDA website for a list of approved tests and testing companies.
- Do not click on links or download files from unexpected emails, text messages, or unfamiliar websites.
- Do not share personal information such as Social Security, Medicare, and credit card numbers in response to an unsolicited call, text, or email.
- Be skeptical of fundraising calls or emails for COVID-19 victims or virus research.

First Choice Bank™
First in Speed | Service | Solutions

Member FDIC

17785 Center Court Drive, Suite 750, Cerritos, CA 90703
(877) 256-9809 or (562) 345-9092
www.FirstChoiceBankCA.com

EQUAL HOUSING LENDER