CYBERSECURITY AWARENESS MONTH

Cybercriminals Are in Love With COVID-19

Cybercriminals know that the best time to turn a phish into a catch is when life gets overwhelming.

They see COVID-19 as a gold mine. In the early days of the COVID-19 pandemic, the volume of fraudulent emails and text messages spiked by more than 667%. And as long as COVID sticks around, scammers will try to use it to their advantage.

What You Can Do

Stay Informed

You can stay current with the latest info on COVID-19 without getting scammed, you just need to be careful. Scammers have created hundreds of thousands of fake "COVID-19" phishing web sites. Make sure you visit only trusted websites such as the Center for Disease Control's official site (https://www.cdc.gov/coronavirus/2019-nCoV/index.html), or your local county or state health department web sites.

If you're unsure about a web site, you can always use this Google tool to see if it's safe: https://transparencyreport.google.com/safe-browsing/search

Be A Little Skeptical

Cybercriminals try to grab our attention with COVID-19-related phishing emails on subjects like these:

- **Contact tracing**. "Someone who came in contact with you tested positive or has shown symptoms for COVID-19. Officials recommend you self-isolate and get tested. More at www.cdc.com/testing."
- **Relief funds**. "The FCC Financial Care Center is offering you $30,000 in COVID-19 relief. Claim at www.fcc.com/relief."
- **Cures**. "Amazing COVID cure discovered. There's hope! Sign-up for the trial here: www.vaccine.covid.co/signup."

Always be wary of emails and offers that are too good to be true.

Stay Cybersafe

Look for the warning signs of someone trying to manipulate you. Dead giveaways include fake URLs, pressuring you to act immediately, urging you to click a hyperlink, or asking you to provide personal or financial information. Remember that government agencies will never call you to ask for personal information or money.