SIX COVID-19 SCAMS

Identity thieves have preyed on the fears, and now the general public fatigue, around the Coronavirus outbreak. Fraudsters continue to exploit opportunities to steal the Personally Identifiable Information (PII), financial information, and even medical information, of those looking for knowledge, protection, and treatment for the viral infection.

What You Need to Know
Beware of the following scams designed to manipulate our fears or take advantage of our fatigue to steal money, personal, and business information:

1. Fake Websites & Online Shopping Scams
Cyberthieves are taking a new twist to earlier COVID-19 scams that have been duping consumers for months. Not only are they creating websites to collect personal information under the guise of providing you with important Coronavirus updates, but also infusing new shopping scams too. Whether they are setting up donation and investment sites for victim support, or online marketplaces that are selling gym equipment or small appliances at “too good to be true” prices, scammers are ready to steal your money and your identity.
If you believe you have purchased a fake item or donated to a fake charity, report it to your credit card company immediately. If you've entered your medical information into a suspicious site, beware of medical identity theft and keep a close eye on all the explanation of benefits you receive to make sure they are legitimate.

2. Phishing and Vishing
As individuals and businesses attempt to keep up with the latest news, they may be more vulnerable to falling for fake Coronavirus update emails, texts, and voicemails that include alerts. Be careful not to click on suspicious links as they may be riddled with malware. As employees frequently check for updates on work conditions, conference and event status, they may be tricked into clicking links that capture sensitive business and customer information. If phone calls request that you share any personal or medical information, just hang up.

3. Spoofed Government and Health Organization Communications
Scammers disguising themselves as government and health organizations such as the World Health Organization (WHO) or the Federal Trade Commission are contacting individuals by email, asking them to visit a “protected” site — requiring personal information to set up a user account — to view safety tips. Or, they are trying to trick recipients into opening email attachments, or are redirecting them to spoofed (or fake) websites and asking for financial details to make donations.
Earlier during the pandemic, cybercriminals hacked into The U.S. Department of Health and Human Services (HHS) and posed as the nation's system to send out text messages warning individuals of a national quarantine and lockdown. The National Security Council posted a Tweet, confirming that the rumors spread by the text message were fake.

Checking for facts directly from the legitimate government organizations is always your best bet, and scam warnings related to Coronavirus and others, are occurring regularly:

- Centers for Disease Control and Prevention (CDC) — https://www.cdc.gov/
- World Health Organization (WHO) — https://www.who.int/
- USA.gov — https://www.usa.gov/coronavirus/
- U.S. Food and Drug Administration (FDA) — https://www.fda.gov/home

4. Testing Fraud

Scammers are marketing fraudulent coronavirus antibody tests and the Federal Bureau of Investigation (FBI) warns consumers they may not only be providing false results, they are also using the tests to collect personal and medical information. Beware of individuals offering “free” antibody tests or providing incentives for undergoing testing. Other signs of fake tests include promotion through social media ads, unexpected emails, or telephone calls posing as government officials requiring a test or requesting personal information to schedule a test. Testing is voluntary, says the FBI, so if you’re being coerced into taking a test you should be extremely cautious as it’s most likely someone trying to steal your PII.

5. Fake Job Postings

Beware of phony job postings designed to recruit individuals who are unemployed or forced to take time off from work during the COVID-19 outbreak. The jobs are created to trick job seekers into becoming money mules and are being posted by scammers who are posing as coronavirus relief charities. After applying for the job, the fake “non-profit” organization will ask the job seeker to process donations made to the charity into their own account and then to transfer the money into another account — all before the bank can alert the individual of the fraudulent check and deposit. Fake job postings not only collect personal information such as name, address, and Social Security number, but also financial account information.

6. Conning Seniors

Scammers are targeting seniors with phone call scams claiming to be fake charities, health organizations offering vaccines, or house cleaning services to help sanitize against the Coronavirus. Check in with your elderly friends and neighbors, to warn them of the tricks scammers are using to steal Social Security checks, and other payments they may be expecting. Strangers may offer to run errands, and then take off with their money. Also, beware of online sellers who advertise hard-to-find cleaning or medical supplies at extreme markups that then never arrive, or say they can “reserve” a COVID-19 vaccine. Remind your loved ones that they should never give out personal, financial, or medical information over the phone (known as vishing scams.)

If you think you are a victim of identity theft, don’t hesitate to reach out to our team here at IdentityForce to learn more about how we can help protect all that you’ve built.

ABOUT SONTIQ

Sontiq is a high-tech security and identity protection company arming businesses and consumers with award-winning products built to protect what matters most. Sontiq’s brands, EZShield and IdentityForce, provide a full range of identity monitoring, restoration, and response products and services that empower customers to be less vulnerable to the financial and emotional consequences of identity theft and cybercrimes. Learn more at www.sontiq.com or engage with us on Twitter, Facebook, LinkedIn, or YouTube.