EZShield®
A Sontiq™ Brand

SIX COVID-19 SCAMS

Identity thieves are playing on the fears of individuals around the world as coverage regarding the Coronavirus outbreak, or COVID-19, increases. Fraudsters are exploiting the opportunity 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 in order to steal money, personal, and business information:

1. Fake Websites

Cyberthieves are creating websites that collect your personal information under the guise of providing you with important Coronavirus updates. They have also set up donation and **investment sites** for victim care or emergency response plans that may seem legitimate, but direct your money into the criminal's pockets.

Fraudulent e-commerce vendors are promoting the sale of **protective face masks**, sanitizers, test kits, and other high demand items — often collecting payment and credit card information without shipping the item. 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.

Most recently, 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**
- Federal Trade Commission (FTC) – **https://www.consumer.ftc.gov/**
- U.S. Securities and Exchange Commission (SEC) – **https://www.sec.gov/investor/alerts**

4. Miracle Cures or Vaccines

The **Federal Trade Commission (FTC)** jointly with the **U.S. Food and Drug Administration (FDA)** warns that there are "no vaccines, pills, potions, lotions, lozenges, or other prescription or over-the-counter products available to treat or cure Coronavirus." All medical advice and treatment should be directed by a medical professional. **False miracle health claims** are a rouse to collect your personal financial and medical details — information that can be used to **commit medical identity theft.**

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 personal financial account information.

6. Not to be Confused for the Beer

Because of its name, people may believe the viral **disease is spread by drinking the popular beer**, Corona. "Coronavirus" is the layman's term for COVID-19. Search trends are showing an uptick in searches for "corona beer virus." Beware of emails or websites that attempt to link the two together, in a humorous or serious way, to get you to enter personal information to reveal more details, jokes, or images.

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

ABOUT SONTIQ

Sontiq, headquartered in Nottingham, MD, 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**.