IT Guidance on COVID-19 Fraud

Warning: Massive Increase in COVID-19 Fraud Schemes

The COVID-19 pandemic has transformed how we work, socialize and do business on an unprecedented scale. This has been accompanied by a massive increase in fraud schemes that prey upon individuals and organizations desperate for equipment and health solutions, particularly through fraudulent coronavirus-related websites, phishing schemes, and malware. Practitioners must take immediate steps to protect themselves, their clients and organisations from COVID-related fraud in all forms.

- **Supply Scams**: Creation of fake websites and shops, social media accounts, and spoofing email addresses to sell in demand medical supplies, like respirators, hand sanitizer, ventilators, gowns, and eye protection.
- **Phishing Emails:** Containing malicious links claiming to be from reputable sources such as Centers for Disease Control Prevention (CDC), World Health Organization (WHO), state governments, etc.
- **Fake Products**: Products claiming to prevent, detect, or cure COVID-19.

Security researchers have tracked a substantial increase in website domain registrations related to COVID-19. Since March, **65,500+ new coronavirus-themed domains have been registered** - most serve up malware or offer fake cures.

Examples:

- **Fraudulent websites selling fake antiviral equipment**.
- Fake **World Health Organization (WHO) vaccine kits or solicitations**.
- **Miracle cure products such as teas, essential oils, colloidal silver, etc.**
- Embedding a bogus **Johns Hopkins Coronavirus Map** to **spread malware, steal sensitive information or extort money**.

How You Can Mitigate the Risk of COVID-19 Fraud

Here is important information to prevent you from being the victim of fraud:

- **Verify the authenticity of websites:**
  - Use **Google Safe Browsing Transparency Report**. Copy and paste the URL and Google will inform you if you can trust that website.
  - Each website has a domain, top level domain (TLD), e.g., **https://www.rescue.org/**

- **Beware of copy-cat domains**; make sure the domain name is correct; e.g., "rescue" and not "rescuenow" and not misspelled "recuee" – misspelling is a common trick.

- **Ensure that website connections are secure with "https"** as in the above; never solely "http".

INTERNATIONAL RESCUE COMMITTEE

This publication was funded by the European Union's Asylum, Migration and Integration Fund

  - **Beware:** hackers are increasingly paying to use “https” – be careful.

- **Independently verify a vendor before purchasing and the authenticity of personal protective equipment (PPE)** by consulting the manufacturer and confirm availability of supplies
.
- **Check online reviews of a company before making a purchase**; e.g., have there been complaints of other customers not receiving the promised items?

- **Be wary of last-minute price changes or excuses for delay in shipment**, unexplained source or solicitation of bulk supply, e.g., PPE, and never provide Personally Identifiable Information (PII).

Report all suspicious emails to your IT department immediately and then delete the message.

Authoritative COVID-19 Resources	
World Health Organization (WHO)	https://www.who.int/
United Nations (UN)	https://www.un.org/
Center for Disease Control (CDC)	https://www.cdc.gov/
International Committee of the Red Cross (ICRC)	https://www.icrc.org/
Johns Hopkins Coronavirus Map	https://coronavirus.jhu.edu/map.html

INTERNATIONAL RESCUE COMMITTEE

This publication was funded by the European Union’s Asylum, Migration and Integration Fund