COVID-19 SCAMS

Counterfeits

Beware of fake masks, hand sanitizer, cleaning products, and preventative "cures". Internet companies such as Amazon, Wal-Mart, Target, etc have been taking down web pages and items off of their shelves. Amazon has a new "Zero Team" which is focused on identifying counterfeits.

Malware

Article at https://www.americanbanker.com/news/coronavirus-scams-to-watch-out-for tells about fake map with embedded malware.

Phishing Scams

Example: Emails with spoofed CDC addresses labeled as Alerts.

Spoofed workplace emails supposedly updating the latest work policy.

Health advice such as how to make your own hand sanitizer.

Emails or links with false, sensational information saying that a celebrity has the virus.

Fraudulent charities asking for donations.

This from Norton.com

Tips for recognizing and avoiding phishing emails

Here are some ways to recognize and avoid coronavirus-themed phishing emails.

Like other types of phishing emails, the email messages usually try to lure you into clicking on a link or providing personal information that can be used to commit fraud or identity theft. Here's some tips to avoid getting tricked.

- **Beware of online requests for personal information.** A coronavirus-themed email that seeks personal information like your Social Security number or login information is a phishing scam. Legitimate government agencies won't ask for that information. Never respond to the email with your personal data.
- **Check the email address or link.** You can inspect a link by hovering your mouse button over the URL to see where it leads. Sometimes, it's obvious the web address is not legitimate. But keep in mind phishers can create links that closely resemble legitimate addresses. Delete the email.
- **Watch for spelling and grammatical mistakes.** If an email includes spelling, punctuation, and grammar errors, it's likely a sign you've received a phishing email. Delete it.
- **Look for generic greetings.** Phishing emails are unlikely to use your name. Greetings like "Dear sir or madam" signal an email is not legitimate.

- **Avoid emails that insist you act now.** Phishing emails often try to create a sense of urgency or demand immediate action. The goal is to get you to click on a link and provide personal information — right now. Instead, delete the message.

Where can I find legitimate information about the coronavirus?

It's smart to go directly to reliable sources for information about the coronavirus. That includes government offices and health care agencies.

Here are a few of the best places to find answers to your questions about the coronavirus.

Centers for Disease Control and Prevention. The CDC website includes the most current information about the coronavirus. Here's a partial list of topics covered.

- How the coronavirus spreads
- Symptoms
- Prevention and treatment
- Cases in the U.S.
- Global locations with COVID-19
- Information for communities, schools, and businesses
- Travel

World Health Organization. WHO provides a range of information, including how to protect yourself, travel advice, and answers to common questions.

National Institutes of Health. NIH provides updated information and guidance about the coronavirus. It includes information from other government organizations.

Good info at: https://www.consumer.ftc.gov/blog/2020/02/coronavirus-scammers-follow-headlines

Here is some info on how to tell if you have a fake product at https://economictimes.indiatimes.com/wealth/spend/how-to-identify-an-original-from-a-counterfeit/articleshow/59398276.cms

Unreal discounts

If you buy something, especially online, at a fraction of the price, or the deal is too good to be true, it usually is. Know how much discount is typically available on branded or luxury items and if the offer is unrealistically low, say, 70-80% of the MRP, then you are definitely buying a fake.

Flimsy packaging

This is a dead giveaway as good brands and businesses take a lot of care and spend a lot of money on packaging. If the item is shabbily packed, doesn't fit properly in the box, uses substandard material like cheap plastic or sagging cardboard, take it as a sign of counterfeiting. Similarly, if you get a product without any packaging at all, know it to be a fake.

Grammatical & spelling mistakes

Counterfeit products can be easily identified through wrong spelling (an extra or a missing letter)

or grammatical errors. For instance, Hewlett Packard will be written as Hewlet, or Louis Vuitton may be spelt as Vitton. While these mistakes in brand names are deliberate to lure the careless customer, those in the product information or instruction manual reflect the fraudsters' lack of education. So read carefully for this clear giveaway.

Fake websites

If you are shopping online, one easy way to counter the purchase of fake items is to check the authenticity of websites. If the site is fake, so are the products. Confirm the URL and ensure that the site is safe by looking for 'https' (instead of http) and the lock sign. You can also verify the site's authenticity by pasting the website address on www.scamadviser.com and http://whois.domaintools.com/. These let you know whether it's a reliable site.

Poor quality of products

The quality of counterfeit products is usually suspect, with cheap alternatives used in place of the original. The material can be tacky plastic, fake leather, cheap glass, poor quality cloth, old or used parts in electronic appliances and gadgets. Even the shape of the containers can be slightly different. If the product has a course, used feel to it, do not buy it.

Omissions & mismatch

The Company prints several features like codes, serial or model numbers, trademark, and patent information on the package or product. Typically, fake products miss out on a few details while copying the information. You can also crosscheck the numbers with the original products online, especially for electronic items or appliances.

Flawed fonts, logos

Much like the spellings, it is easy to detect fake logos, brand names and trademarks, if you are paying attention. If you are observant and know the original logos well, you can catch even the smallest variation. If this is difficult for you, take a picture of the product you think is fake, and compare it with the original online. The font could be slightly different or of the wrong size. Even the coloring could be faded or altered minutely from the original. The printed text could be faded, smudged, illegible or misaligned.

No contact details

If the manufacturer's physical address, e-mail, phone number or contact details are not listed on the product or package, it should be cause for concern. This implies you have no means of contacting anyone for grievance redressal. It is best to avoid such products. If the contact details are mentioned, try to verify these on the website or call to confirm before you make a purchase.

Missing accessories

Make sure that all the supplementary parts and accessories that have been mentioned on the package are present in the box. If the instruction manual, warranty card, wires, plugs or other items are missing, get back to the retailer immediately. Better still, open the box and check it in the store before buying. In case of an online purchase, make a video recording of the unboxing

while taking delivery.

Unauthorized centers

It’s best to buy electronic items, appliances, gadgets and branded ware from authorized retailers, licensed sellers and genuine brand outlets. If you are getting a good discount elsewhere, check the store’s address by going online and make sure you have genuine contact details.