Information piracy attacks under the Corona pandemic

Corona pandemic, a large group of hackers of information on the Internet and social media, has exploited the need of individuals to know the details of this pandemic such as its symptoms and repercussions and methods of treatment in order to implement its goals by hacking computers and seizing data, for individuals and institutions.

What the attackers are doing is designing websites related to the Corona virus, and they require users to download the application to keep them informed of the situation using malware, without a doubt reviving the emerging corona virus, piracy and fabricating news and information on the Internet and social media, in light of the trauma of the "Corona virus".

Malicious programs

What hackers and information hackers do is distribute emails, booby-trapped malware, as if they were educational flyers about the Corona virus, and the texts of these messages, to open an attached file to learn more about the virus. The attached files allow hackers to access the victim's computer, thereby hacking personal data, or destroying and disabling computer software, sometimes bargaining and asking for ransom.

Other malicious e-mail messages that appear to originate from the World Health Organization, asking recipients to provide them with sensitive information or clicking on malicious links. The World Health Organization was aware of the malicious e-mails exploiting the emergency with the emerging corona virus, and warned them, but the problem was that it could not prevent it Or stop it.

Phishing protection

Phishing is an attack that is designed to steal your money, or your identity, by getting you to divulge personal information on websites that pretend to be legitimate sites. These websites are designed to lure you into revealing personal information, such as credit card numbers, bank information, or passwords. Cybercriminals typically pretend to be reputable

companies, friends, or acquaintances in a fake email message, which contains a link to a phishing website.

Some examples of messaging in these emails are:

- Emails that promise a reward. “Click on this link to get your tax refund!”
- A document that appears to come from a friend, bank, or other reputable organizations. The message is something like “Your document is hosted by an online storage provider and you need to enter your email address and password to open it.”
- An invoice, or shipping notice, from an online retailer or supplier for a purchase or order that you did not make. The attachment appears to be a protected or locked document, and you need to enter your email address and password to open it.

COVID-19 being exploited by attackers

Currently we're seeing a lot of phishing and scam emails claiming to be related to the COVID-19 outbreak, or government financial relief programs, and from legitimate sources like the government, medical facilities, or banks.

Learn to spot a phishing email

Phishing is a popular form of cybercrime because of how effective it is. Cybercriminals have been successful using emails to get people to respond with their personal information. The best defense is awareness and knowing what to look for.

Here are some ways to recognize a phishing email:

- **Urgent call to action or threats** - Be suspicious of emails that claim you must click, call, or open an attachment immediately. Often they'll claim you have to act now to claim a reward or avoid a penalty. Creating a false sense of urgency is a common trick of phishing attacks and scams.
- **Spelling and bad grammar -** Cybercriminals are not known for their grammar and spelling. Professional companies or organizations usually have an editorial staff to ensure customers get high-quality, professional content. If an email message has obvious spelling or grammatical errors, it might be a scam.
- **Suspicious links -** If you suspect that an email message is a scam, do not open any links that you see. Instead, hover your mouse over, but don't click, the link to see if the address matches the link that was typed in the message. In the following example, resting the mouse on the link reveals the real web address in the box with the yellow

background. Note that the string of IP address numbers looks nothing like the company's web address.

- **Mismatched email domains -** If the email claims to be from a reputable company, like Microsoft, but the email is being sent from another email domain like Yahoo.com, or microsoftsupport.ru it's probably a scam. Also be watchful for very subtle misspellings of the legitimate domain name. Like micros0ft.com where the second "o" has been replaced by a 0, or rnicrosoft.com, where the "m" has been replaced by an "r" and a "n". These are common tricks of scammers. This is very similar to the next tip...
- **Altered web addresses -** A form of spoofing where web addresses that closely resemble the names of well-known companies, but are slightly altered; for example, www.micorsoft.com or www.mircosoft.com.
- **BCC -** The mail is sent to multiple recipients or to you in BCC.

Cybercriminals can also get you to visit fake websites with other methods, such as text messages or phone calls. Sophisticated cybercriminals set up call centers to automatically dial or text numbers for potential targets. These messages will often include prompts to get you to enter a PIN number or some other type of personal information.

- **Outlook.com**. If you receive a suspicious email message that asks for personal information, select the check box next to the message in your Outlook inbox. Select the arrow next to **Junk**, and then point to **Phishing scam**.
- **Microsoft Office Outlook 2016 and Outlook for Microsoft 365**. While in the suspicious message, select **Report message** in the **Protection** tab on the ribbon, and then select **Phishing**.

If you receive an unsolicited phone call, take down the caller's information and report it to your local authorities.