NOUVEL HAY MAGAZINE
SANS FRONTIÈRES

Les cybercriminels exploitent le Covid-19 …

Cybercriminals are exploiting the COVID-19 pandemic to perpetrate fraud

Cybercriminals are exploiting the COVID-19 pandemic to perpetrate fraud

As more people are working from home, cyber criminals are exploiting the COVID-19 pandemic to target organizations and individuals with sophisticated fraud scams. The FBI recently announced a rise in fraud schemes[1] related to the COVID-19 pandemic.[2] Organizations may find themselves more vulnerable due to their remote workforce and limited staff. It is important to stay vigilant to help protect yourself from increased fraud risks resulting from the virus impacts.

Phishing and malware attacks are on a steep incline. Barracuda Network researchers have reported an increase of 667% in COVID-19 related phishing attacks since the end of February.[2] Criminals posing as legitimate organizations send emails and text messages that lure potential victims into disclosing sensitive data, such as passwords, personally identifiable information, and bank account details. Using malware, fraudsters can swiftly gain access to your computer to monitor and record your keystrokes or inject ransomware. Cyber criminals are using information in the news about COVID-19 to design their attacks, such as targeting remote workers with emails that notify them of a positive COVID-19 test within their organization.

Ransomware is becoming increasingly popular as cyber criminals seek bigger ransom payoffs knowing that many companies are vulnerable while operating in these challenging times. In a ransomware attack, fraudsters hold your computer or network hostage, blocking access to your data and important files until you pay a large sum of money. All sectors are at increased risk for ransomware, but healthcare and government agencies may be at higher risk because cyber criminals know how critical those services are right now.

Impostor fraud, also known as business email compromise (BEC), is a significant threat to your business. BEC is where a fraudster impersonates a vendor, a company executive, or another trusted trading partner — ultimately tricking you into making the payment to them. Organizations that are unable to consistently adhere to standard operating controls and procedures because of staffing shortages and an increasingly remote workforce may be especially vulnerable to BEC. Employees should be on the lookout for medical supply scams, and fraudulent donation sites that may impersonate a company, charity, or government agency to convince them to make purchases or donations on spoofed websites or do business with a phony vendor.

Finally, **account takeover** is another serious fraud threat that is on the rise due to the recent increase in phishing attacks and distribution of malware. With account takeover, thieves gain access to make unauthorized transactions, including transferring funds, creating and adding fake employees to payroll, and stealing sensitive customer information. Organizations especially at risk are those who may not have a robust work-from-home program and well-established security controls.

Take the following precautions to help protect your organization's assets

- **Beware of increased phishing attacks**
  It is especially important during these times to avoid clicking links or opening attachments from suspicious or unknown senders, and use caution when visiting untrusted websites, which may be contaminated with malware. Keep your antivirus and anti-spyware software and firewalls updated regularly. If possible, use separate devices for your work activities and personal activities to limit your exposure to phishing attacks.

- **Strengthen and follow your internal controls for payments**
  As your company shifts to a remote workforce, ways to mitigate vulnerabilities include: using dual custody for all online payments (ACH, wire transfer, foreign exchange) and administration services, reconciling accounts daily to detect suspicious activity, and locking check stock and signature stamps in a secured location.

- **Verify your payment information**
  Always verify payment requests and changes to payment instructions. Make sure that requests to change payment details, such as account or invoice information, are authentic. Verify the request using a different method of contact. For example, if the vendor contacts you by email, confirm the information by phone. Be sure to use the information you have for the contact on file, not the contact information contained in the request you received. Ensure your employees have access to trusted vendor phone numbers on file, especially when working remotely, to facilitate call backs to confirm payments. Be extremely cautious so you can spot medical supply scams and fraudulent donation sites — do your research to help ensure you are working with a legitimate vendor or organization.

- **Protect access to your sign-on credentials and beware of unexpected token prompts**
  Never give out passwords, IDs, token codes, or other authorization credentials. Be cautious of unexpected token prompts. Ignore pop-ups seeking your online banking sign-on credentials. Be wary of unsolicited calls, including from your bank, to assist you with sign-on issues you didn't report.

- **Don't sign on to your account from a link in a suspicious message**
  Always access websites by using a reputable search engine or entering the entire URL into your browser. Do not use the same passwords on multiple websites.

- **Improve your remote access security program**
  Remote workers may introduce greater cybersecurity risks due to internet security settings at home. Employees may expose company devices to additional risk as they leave the safety and security of the workplace. Work with your IT team to reevaluate your work-from-home program, and work with employees to ensure their home internet connections are secure.

Fraud attacks are inevitable for most businesses, and cyber criminals are exploiting the COVID-19 pandemic to perpetrate even more fraud scams.

Make sure you educate your employees and partners on the increased fraud risks arising from COVID-19 and how to stay vigilant against fraud attacks.

[1] **FBI sees rise in fraud schemes related to the Coronavirus (COVID-19) pandemic**