The Online Frontline | Vol. 01

First Data is now fiserv.

Defending against COVID-19 cyber scams

As you may have seen, recent news stories have been filled with reports of coronavirus-themed cybercrimes. Considering just the volume of threats so far, the pandemic could become the largest cybercrime theme of all time.

Unfortunately, many threat factors are capitalizing on the panic and discomfort of the COVID-19 pandemic, as well as, the stay-at-home orders and long-term reliance on digital technologies and services, in order to conduct special-crafted malware and phishing attacks worldwide.

We're seeing a steep uptick in phishing scams and other weaponized email attacks that play on the fear and uncertainty surrounding COVID-19 to steal credentials and spread malware. Bad actors are posing as the World Health Organization and the Centers for Disease Control and Prevention, using fake government relief checks as bait and touting fake COVID-19 tracking apps.

Criminals are also targeting businesses with more specific attacks, such as fake IT help desk messages and internal corporate emails. Businesses should make sure all employees, as well as any susceptible consumers, are aware of those coronavirus-themed scams and the best practices to avoid falling victim to one. There are many types of lures used to deploy the same types of attack vectors – the means by which a hacker can gain access to a computer or network server – to exploit system vulnerabilities.

Cybersecurity at Fiserv is dedicated to cyber-preparedness and data-centric defense strategies in order to stay ahead of the attack methods and technologies that have rapidly evolved. With our mission to protect data, Fiserv encourages professionals and businesses to be doubly vigilant and take the following precautions during these uncertain times.

Maintaining security for remote workers

Remote workers should ensure their home routers have strong, unique passwords and are running the latest firmware. If possible, they should use a dedicated workstation for all business activity.

- If remote workers must use personal devices, IT staff should verify that antivirus software and any other available safeguards are installed and up to date
- Employees should store business data only in designated secure locations
- Strong encryption should be used for transmitting Business Confidential Information (BCI), Personally Identifiable Information (PII) and other sensitive data elements that require protection

Use Virtual Private Networks

Virtual Private Networks (VPNs) are valuable tools for protecting business communications and data when working remotely, and there has naturally been a huge jump in VPN use due to COVID-19. However, it's critical to use a VPN solution that's a good fit for your company and, above all, trustworthy.

The top priorities

The most important controls are:

- Using a secure email gateway system that includes inspection and sandboxing of incoming messages. Strong controls can prevent the majority of threats from making it to your end-user technology
- Applying up-to-date and effective endpoint security to protect corporate networks when accessed through remote devices. Behavioral and signature-based systems should ensure incident response teams can remotely access, respond, investigate and quarantine any threats that are not automatically handled by the endpoint's built-in functions
- Relying on strong internet proxy monitoring and filtering of malicious sites with regularly updated intelligence. Blocking an endpoint from calling out to download malware or instructions from a ransomware threat is critical
- Using authenticated email. Make sure your clients can feel secure that an email sent by a member of your team is legitimate. Using a Sender Policy Framework and DomainKeys Identified Mail email protection helps prevent the delivery of malicious email messages to clients
- Relentlessly educating your workforce on threats and instituting a reporting mechanism to allow associates to report and send suspicious messages instantly to your security teams for review and action

Professionals must be doubly vigilant

While COVID-19 has forced many workers to pause or drastically alter their routines, businesses should strive to give these professionals the support and resources they need in these tumultuous times.

Now more than ever, good cybersecurity must extend beyond conventional approaches. This more complex and perilous threat landscape makes big data tools and a data-centric defense strategy even more essential. With more work being done remotely, strong cyber and tech units with efficient and collaborative work environments will be more valuable.

Businesses will need to be proactive in finding the best cybersecurity professionals for their teams because talent is going to be in higher demand than ever before. But with the right priorities, practices and people in place, workforces will be able to securely connect, communicate and carry on.

Ready to better protect data and build digital trust?

Visit **FirstData.com/Security** or contact us at **cybersecurityproductteam@FirstData.com** or call **1-866-8330** to learn more.

FirstData.com

653181 2020-4