Vishing Scheme Posing as FIS Tech Support

7/14/2021

What Is the Issue?

Some FIS clients may have been targeted by criminal actors conducting a vishing (voice phishing) attack claiming to be "FIS Tech Support" and using a spoofed telephone number of 800.215.8260. The actor claims to be calling for a "system update" and asks the employee to go to a site to "check network speed." Currently, it is unknown what website the actor wants them to visit or the intent of the campaign.

What Is FIS' Response?

FIS' Cyber Threat Intel (CTI) team has been working with the client that reported this issue to gather more information; however, we do not have enough data at this time to fully investigate the issue. We are taking this threat seriously as it closely resembles a joint advisory issued by the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) in August 2020.

> *Actors first began using unattributed Voice over Internet Protocol (VoIP) numbers to call targeted employees on their personal cellphones, and later began incorporating spoofed numbers of other offices and employees in the victim company. The actors used social engineering techniques and, in some cases, posed as members of the victim company's IT help desk … to gain the trust of the targeted employee. The actors then convinced the targeted employee to visit a malicious link.*

FIS CTI has shared this information with the Financial Services Information Sharing and Analysis Center (FS-ISAC) and clients. FIS will continue to monitor for new intelligence related to this threat and respond appropriately.

What Should You Do?

Be alert to suspicious or unsolicited phone calls about system updates claiming to be from a legitimate organization. Do not go to any websites provided by the caller or provide information about your organization unless you are certain of a person's authority to have the information. If possible, try to verify the caller's identity directly with FIS first. Should you receive one of these calls, document the phone number of the caller as well as the domain that the actor tried to send you to and contact Client.Risk.Relations@fisglobal.com.