STC Fraud News

September 2018

All About Tech Support Scams

Statistics show that every 10 seconds another unsuspecting person becomes a victim of a Tech Support Scam. These scams grab the victims attention in a variety of ways, but the two most popular are from a telephone call or through a pop up screen on the victim's computer.

Telephone Scams: The victim receives a call from "Microsoft" or "Dell" claiming to be Tech Support and baiting the victim by telling them that there is a virus on their computer and they need to remote in to the computer in order to fix it. Hopefully, the victim hangs up but unfortunately about 3.3 million people fall for this scam every year.

Pop Up Screen: While the victim is on the computer they get a pop up that might say WARNING! Your computer may have a virus! Click here for help or call us for assistance! Again, we hope the customer does not take the bait, but given the $1.5 billion dollars a year lost to these scams, they click or call more often than not.

Now, let's take a look at some of the issues that may stem from a Tech Support Scam:

Money Lost by Paying for a Fake Service: While the "tech support employee" is remoted into the computer, they mention there is a fee for fixing the problems. Most scammers start out by saying that it will cost $29.99 (or maybe more!). Then, during the phone call the scammer has found "so many viruses and malware, that there is an additional charge to have it fixed." At this point we have seen the scammer charge anywhere from an additional $50 to $900. There have even been instances where a victim is instructed to purchase gift cards and relay the numbers to the scammer. Check out the Online Banking section for a more in depth example of how a victim can lose money!

Viruses/Malware and Key Loggers: Most likely, when a victim received the phone call or a pop up stating that their computer has a virus, there really aren't any problems. The real issues start *after* the victim allows the "support" person to login. At this point, they begin to install viruses, malware and key loggers. These programs track what you do on the computer, slow it down and could end up costing a lot more money in the future to have a reputable service clean the computer (or in some cases, to buy a new one!) The scammers can also watch the activity done on the PC, see user names and passwords are for different websites, access email accounts and more!

Online Banking Risks: Once these scams begin, there are programs placed on the PC that can watch the user's internet activities. This includes seeing the login info for online banking and the information inside, such as account balances. Once the scammer gains access to online banking they can initiate wire transfers, change addresses, sign up for Bill Pay and more! We have received fraudulent wire requests stemming from a text scam up to $11,000! With online banking access, a scammer may also initiate a transfer between accounts, for example, they may transfer $3000 from an Easy Access Loan or savings account to the checking account. Then the scammer tells the victim that they accidently initiated a refund instead of debiting their account for the service. So, instead of charging them $300 to clean the computer, they "credited" the account $3000 in error. If the victim only looks at the balance in their checking, it seems as if the scammer is telling the truth! To fix the error, the scammer instructs the victim to send the "refund" back via MoneyGram, Western Union or by purchasing gift cards. If the victim does not realize the money was transferred from their own account in time, they could end up losing thousands of dollars. We have seen fraudulent transfers of up to $8000 occur.

Continued on page 2...

E-mail and Social Media Hacking: Once a scammer is in a PC, they have access to email and social media accounts. Many times, this is where the hacker will send out emails appearing to be from the victim with links to click on (ex. Check out pics from my vacation! Click here to see my albums!), which leaves friends and family vulnerable to scams as well. A social media hack might include the scammer creating a duplicate profile and impersonating the victim. Many times, the scammer will end up communicating with friends and family that the victim doesn't speak with often, swapping stories and getting close with them. They eventually come up with a story of financial hardship and try to get the friend or family member to send money to help.

Identity Theft Risk: Think about everything you do on your computer. Do you pay bills? Do you login to your credit card site to pay it, change an address, and redeem reward points? Do you do file taxes on Turbo Tax? Do you save those tax returns to your PC? A computer can house SO much more than just pictures or the occasional game of solitaire. PCs are often a treasure trove of personal information that scammers can use to commit various forms of identity theft. They could login to a credit card accounts, change the address and request a new card or credit increase.

There have been cases where a scammer logged into a victims cell phone account to change the address and order a new phone, and one where the scammer ported the victim's number to a different service in an effort to drain a Bitcoin account.

CATO (Corporate Account Take Over) Risk: Business computers often house a TON of information. If a scammer is able to remote into a business computer *or a personal computer that houses business information*, the impact can be significant. If the computer they compromise is used to process payroll, that could expose names, addresses, phone numbers, account and routing numbers, and social security numbers of employees! If they gain access to a computer used to process invoices, that could expose customer payment information (account numbers, debit card numbers etc.) the scammer could even send out fake invoices. Think about your computer. What could a scammer see and gain access to if they were to hack your PC? You are your own best defense, be careful what you click on!

The Bottom Line: Scam artists are finding new ways every day to entice victims. If you feel you are the victim of a scam, notify the bank immediately! Somerset Trust Company's People First Call Center is available M-F from 7am-9pm and Saturday-Sunday from 7am-5pm at (800) 972-1651. We also offer a Fraud Hotline you can call M-F 8am-4:30pm which you can reach at (814)530-1013 .

Fraud Outreach Program

Somerset Trust Company offers a FREE Fraud Outreach program to customers and non customers. A representative from STC will visit any group of people (ex. Church Group, Non Profit, Business, etc) and discuss fraud trends, identity theft and more. We can customize the presentation to your group in an effort to keep everyone interested and engaged. Again, you are your best defense against fraudulent activity. The more you know about different scams, the better equipped you are to avoid scam artists and fraudulent activity. To schedule a Fraud Outreach Presentation, visit your local branch or contact our Call Center and ask to speak with Angie Rowland in Marketing.

If you have any questions, comments or suggestions about this newsletter, we would love to hear from you! Please contact:

Angela Corrigan

Fraud/CATO Officer

(814)443-9394

Corrigan@SomersetTrust.com