TACTICS SCAMMERS USE TO TRICK YOU

SLVCC 2023

ALWAYS BE AWARE

- SCAMMERS ARE KNOWN FOR PREYING ON VICTIMS' VULNERABILITIES, SUCH AS FINANCIAL HARDSHIP, FEAR, AND CONFUSION. PEOPLE WHO BELIEVE THEY ARE SAVVY ENOUGH TO AVOID SCAMS MAY STILL FALL VICTIM, NONETHELESS.
- PROACTIVE EDUCATION IS THE BEST WAY TO PROTECT YOURSELF.
- HERE ARE COMMON PRACTICES SCAMMERS KEEP IN THEIR ARSENALS TO ATTEMPT TO FOOL YOU AND COMMIT FRAUD.

FAKING AN EMERGENCY

- SCAMMERS PRETEND TO REPRESENT AN OFFICIAL ORGANIZATION (LIKE THE IRS) AND CALL, TEXT, OR MAY EMAIL YOU TO DEMAND IMMEDIATE MONEY FOR BOGUS ISSUES.
- THEY USE THREATENING PHRASES SUCH AS, “YOUR 401K PLAN WILL BE FROZEN,” “YOUR PASSPORT WILL BE SEIZED,” OR “THE MAXIMUM SENTENCE FOR THIS CRIME IS FIVE YEARS IN PRISON AND A $10,000 FINE,” TO CATCH POTENTIAL VICTIMS OFF GUARD AND CREATE A SENSE OF URGENCY.
- EXPRESSING RESISTANCE IS INEFFECTIVE. ONCE THE SCAMMER HAS CREATED THE EMERGENCY AND INSTILLED PANIC, THEY REINFORCE THERE IS NOTHING YOU CAN DO TO REMEDY THE SITUATION.
- IN THE CASE OF AN IRS SCAM, THEY MAY SAY YOU MUST COOPERATE OR FACE ARREST AND/OR FINES.

REWARDING COOPERATION

- SCAMMERS SOMETIMES TRY TO PLAY THE PART OF A TRUSTED FRIEND, OFFERING HELP AND A WAY OUT OF THE EMERGENCY THAT WOULD PROVIDE YOU RELIEF.
- THEY MIGHT EVEN TELL YOU THAT YOU SEEM LIKE A GOOD PERSON AND OFFER TO HELP YOU WITH THE SITUATION AT HAND.

KEEP YOU ON THE PHONE

- NOT ALLOWING VICTIMS TO HANG UP UNTIL THEY PAY UP.
- PHONE SCAMMERS SAY IT IS A ONE-TIME OPPORTUNITY FOR YOU TO TAKE ACTION TO AVOID FURTHER CONSEQUENCES, AND IF YOU HANG UP THE PHONE, YOU WILL NOT BE OFFERED ANOTHER CHANCE TO RESOLVE THE PROBLEM.

IMPRESSIVE TITLES

- SCAMMERS TRY TO SOUND IMPRESSIVE TO GAIN YOUR TRUST.
- THEY USE OFFICIAL-SOUNDING TITLES AND NAMES FOR MERCHANTS AND EVERYDAY ITEMS. EXAMPLES INCLUDE REFERRING TO A GIFT CARD AS AN “ELECTRONIC FEDERAL TAX PAYMENT SYSTEM,” OR INSTEAD OF USING THE NAME OF A STORE, THEY CALL IT A “GOVERNMENT-AFFILIATED PAYMENT PROCESSOR.”

THEIR APPROACH

- SCAMMERS KNOW ASKING FOR PERSONAL INFORMATION SHOULD RAISE ALARM BELLS.
- INSTEAD, THEY MAY SAY THEY ARE NOT LOOKING TO OBTAIN THIS INFORMATION, OR THEY ARE NOT LOOKING FOR AN EXCHANGE OF FUNDS OVER THE PHONE, WHICH IS DESIGN TO MAKE YOU LET DOWN YOUR GUARD.
- THIS IS WHY SCAMMERS OFTEN USE GIFT CARDS TO EXTRACT PAYMENT.
- YOUR FINANCIAL INSTITUTION WILL NEVER CALL YOU AND ASK FOR PERSONAL INFORMATION (THEY ALREADY HAVE A LOT OF IT). IF A CALLER DOES, HANG UP.

ADDED ASSURANCE

- IN AN ATTEMPT TO SOUND LEGITIMATE, SCAMMERS SAY THE CALL IS BEING RECORDED AND MONITORED BY THE IRS OR SOMETHING ELSE.

THREATENING TO ALERT THE MEDIA

- SCAMMERS GO TO GREAT LENGTHS TO KEEP SUSPICIOUS OR WARY POTENTIAL VICTIMS ON THE PHONE, AND EVEN GO SO FAR AS TO THREATEN TO CONTACT THE MEDIA ON BEHALF OF THE IRS IF YOU DO NOT COMPLY WITH WHAT IS BEING ASKED.
- THIS IS USED AS A LAST RESORT TO SALVAGE A CONVERSATION THAT MIGHT NOT BE GOING WELL.

EXPLOITING YOUR CONFIDENCE

- ONCE SCAMMERS HAVE YOU HOOKED, THEY MAY TRANSFER THE CALL TO ANOTHER FAKE AGENT IN AN ATTEMPT TO FURTHER LEGITIMIZE THE CALL.
- OFTEN, THESE SCAMMING “CALL CENTERS” EMPLOY MULTIPLE SCAMMERS WHO WORK TOGETHER TO MAKE THE INITIAL CALL AND THEN CLOSE THE SCAM.
- SCAMMERS ARE HIGHLY ORGANIZED: SOME ARE RESPONSIBLE FOR GETTING POTENTIAL VICTIMS HOOKED, WHILE OTHERS FOCUS ON CLOSING THE DEAL BY EXTRACTING PAYMENT.
- THEY MAY SAY, “PLEASE HOLD ON THE LINE, I AM TRANSFERRING THE CALL TO MY SENIOR TREASURY SPECIALIST,” OR “THANKS FOR WAITING, THIS IS SENIOR OFFICER MATTHEWS FROM THE ACCOUNTING DEPARTMENT. MY BADGE ID IS…”

SECRECY

- INSISTING YOU KEEP QUIET ABOUT SPECIAL OFFERS OR THE SITUATION.
- IF A SCAMMER OFFERS A SPECIAL TAX BREAK, FOR INSTANCE, THEY WILL OFTEN DEMAND THAT YOU NOT DISCUSS IT WITH ANYONE, AS IT WOULD PREVENT YOU FROM RECEIVING THE SETTLEMENT.

OTHER TACTICS YOU SHOULD AWARE OF

- YOU MAY BE GUIDED TO SAY SPECIAL WORDS .
  - IF A SCAMMER HAS A RECORDING OF YOU SAYING THE WORD YES, THEY CAN USE IT TO FOOL YOUR BANK AND RIP YOU OFF. SO DO NOT ENGAGE WITH AN UNKNOWN CALLER BY ANSWERING YES TO ANY OF THEIR QUESTIONS. CONSIDER SAYING ALTERNATIVES LIKE “CORRECT”, “ALRIGHT”, “POSITIVELY”, “INDEED”.
    - HELLO, I’M TOMMY WITH XXXXXXX. AM I SPEAKING WITH ANITA? **“CORRECT” NOT “YES”.**
  - YOU MAY ALSO BE REQUESTED TO SAY YOUR COMPLETE NAME FOR SECURITY REASONS. **“DON’T”**
  - RATHER THAN HELLO, CONSIDER - “CAN I HELP YOU”, “GOOD AFTERNOON/MORNING/EVENING”

IN SUMMARY – WHAT TO WATCH FOR

- 1. SCAMMERS PRETEND TO BE FROM AN ORGANIZATION YOU KNOW OR ARE FAMILIAR WITH.
- 2. SCAMMERS SAY THERE'S A PROBLEM OR A PRIZE.
- 3. SCAMMERS PRESSURE YOU TO ACT IMMEDIATELY.
- 4. SCAMMERS TELL YOU TO PAY IN A SPECIFIC WAY.
- 5. SCAMMERS TRY TO GET YOU TO FOLLOW LINKS TO THEIR FAKE "SCAM" SITES OR "OFFICE" NUMBERS VIA EMAILS.

IN SUMMARY – WHAT TO DO

- BLOCK UNWANTED CALLS AND TEXT MESSAGES.
- DON'T GIVE YOUR PERSONAL OR FINANCIAL INFORMATION IN RESPONSE TO A REQUEST THAT YOU DIDN'T EXPECT.
- RESIST THE PRESSURE TO ACT IMMEDIATELY.
- KNOW HOW SCAMMERS TELL YOU TO PAY.
- STOP AND TALK TO SOMEONE YOU TRUST.
- ALWAYS USE YOUR BANKING APP, WEBSITE. (NEVER A LINK). USE THE PHONE NUMBER OFF THE WEBSITE (NEVER FROM YOUR CALLER-ID).

REPORT YOUR ENCOUNTER

- HTTPS://REPORTFRAUD.FTC.GOV
- HTTPS://WWW.USA.GOV/WHERE-REPORT-SCAMS
- HTTPS://WWW.FBI.GOV/HOW-WE-CAN-HELP-YOU/SCAMS-AND-SAFETY/COMMON-SCAMS-AND-CRIMES
- HTTPS://CONSUMER.FTC.GOV/SCAMS

WE WILL POST THESE ON OUR SLVCC WEBSITE