

“THE WILD WEST” YOUR COMPUTER/INTERNET/PHONE, ANY PHONE!

SOCIAL SECURITY NOW ADVERTISES ON ITS ENVELOPES : SCAM ALERT (SCAMMERS ARE PRETENDING TO BE GOVERNMENT EMPLOYEES. THEY MAY THREATEN YOU AND MAY DEMAND IMMEDIATE PAYMENT TO AVOID ARREST OR OTHER LEGAL ACTION. DO NOT BE FOOLED!

IF YOU RECEIVE A SUSPICIOUS CALL: #1 HANG UP! #2 DO NOT GIVE THEM MONEY OR PERSONAL INFORMATION! #3 REPORT THE SCAM AT OIG.SSA.GOV

IRS HAS SIMILAR SITUATIONS, THEY WILL NOT CALL YOU ON THE PHONE, IT IS HARD ENOUGH TO CALL THEM!

YOUR BANK HAS ALL YOUR INFORMATION, IF SOMEONE CALLS AND ASKS FOR PERSONAL INFORMATION, IT IS NOT YOUR BANK!

AARP BULLETIN HAD AN EXCELLENT ARTICLE IN THEIR OCTOBER 2023 ISSUE VOL 64 “A VISUAL GUIDE TO FRAUD”

LOOK FOR SIGNS THAT YOU ARE BEING STALKED BY CROOKS:

- 1. TEXTS FROM STRANGERS, DO NOT RESPOND, DELETE AND MARK AS JUNK.**
- 2. TEXT ABOUT YOUR NETFLIX ACCOUNT BEING SUSPENDED, DO NOT RESPOND DIRECTLY, THEY ARE FISHING FOR INFO.**
- 3. CAR WARRANTY OFFERS, NOT REPUTABLE**
- 4. FAKE BUSINESS EMAILS; FROM MAJOR RETAILER ON LINE, DO NOT RESPOND THRU THE EMAIL, YOU CONTACT DIRECT**
- 5. GIFT CARDS HAVING YOU PAY FOR ANYTHING WITH YOU SENDING THEM THE CODES OFF THE CARD.**
- 6. SOCIAL MEDIA FRIEND REQUESTS, DO NOT GET INVOLVED WITH STRANGERS**
- 7. POP UP ADS CAN DOWN LOAD MALWARE TO YOUR DEVICE**
- 8. COMPUTER VIRUS ALERTS, NEVER CALL A NUMBER LISTED OR CLICK ON LINK, HIRE A KNOWN COMPUTER TECH**
- 9. PHONE CALLS FROM NUMBERS LIKE YOURS, FALSE CALLER ID NAMES ON DISPLAY**
- 10. QR CODE DIRECTING YOU TO A CRYPTO ATM: JUST FORGET ABOUT CRYPTO! SPEND YOUR MONEY ON YOURSELF.**

OUR WORLD IS GETTING MORE CONVENIENT, BUT THAT COMES WITH A COST, YOUR SECURITY. MOST OF THE DANGERS ARE INSIDE YOUR HOUSE. WE CONSTANTLY HEAR THAT MAKING DIFFICULT PASSWORDS WILL PROTECT YOU, WHICH RESULTS WITH TOO MANY TO REMEMBER, YOU GET A SECURITY PROGRAM TO STORE YOUR INFO ON THE INTERNET WHERE ALL THE CRIME RESIDES. THE MOST DANGEROUS SITUATION IS DUE TO THE GATEKEEPER (YOU), BY ANSWERING THE PHONE, CLICKING ON AN EMAIL OR OPENING ATTACHMENTS.

RECENTLY WE HAVE BECOME AWARE OF AN INSIDIOUS SCAM THAT DRAWS THE UNSUSPECTING AND EVEN THOSE WHO QUESTION THE SITUATION INTO A WEB. WE LIKEN IT TO A DOUBLE BLIND CONFIRMATION, A CALL OR EMAIL FROM A POSSIBLE RELATION, BANK, PENSION, BROKER, GOVERNMENT AUTHORITY. YOU MIGHT BE CAUTIOUS OF THIS CALL, BUT THEY MIGHT WARN YOU THAT YOU HAVE BEEN HACKED AND TO NOT USE YOUR PHONE FOR OUTGOING CALLS AND THAT A BANK EMPLOYEE OR GOVERNMENT EMPLOYEE, MAYBE EVEN SOCIAL SECURITY WILL CALL YOU SHORTLY TO EXPLAIN THE SITUATION IN MORE DETAIL. THE DRIVE FOR THIS ACTION IS TO SCARE YOU AND PUT YOU ON AN ISLAND ALL BY YOURSELF AND SOMEONE WILL COME TO SAVE YOU. THEY ARE "TAG TEAMING" YOU TO MAKE YOU THINK THAT THEY ARE HELPING YOU. REMEMBER, THEY STARTED THE STORY TO BEGIN WITH SO CUT OFF THE CONVERSATION IMMEDIATELY! IF THERE IS A REAL PROBLEM, THEY WILL MAIL YOU CORRESPONDENCE. THE INTERNET AND ALL ACCOMPANING SERVICE IS THE "WILD WEST" ENTER AT YOUR OWN RISK, BUT BE AWARE THAT YOU ARE THE MARK.

ANYONE WHO FALLS PREY TO ONE OF THESE SCAMS CAN BE SUBJECT TO ANOTHER SUCH CALL TO GET A SECOND BITE OF THE APPLE, YOU ARE THEN MARKED AS "EASY PICKINGS".

Barry B. DeMarr

Bryan F DeMarr