PROTECT YOUR PERSONAL INFORMATION:

FTC.GOV – REQUEST A FREE CREDIT REPORT ANNUALLY. REVIEW IT AND ANY ACCOUNTS NOT RECOGNIZED, CONTACT THE FINANCIAL INSTITUTION AND CLOSE IT AND REPORT THE ACCOUNT AS FRAUD TO THE CREDIT BUREAU AND HAVE IT REMOVED.

USE 1 COMPUTER FOR YOUR BANKING TRANSACTIONS ONLY, A SECOND FOR PERSONAL USE WEB SEARCHES ETC.

WHEN PAYING BILLS ON LINE, NEVER USE THE HYPERLINK – USE THE FINANCIAL INSTITUTIONS ACTUAL "OFFICIAL" WEB SITE.

ALWAYS CLEAR WEB BROWSER HISTORY AND CACHE.

WHEN FILLING OUT PATIENT INFO AT THE DOCTORS OFFICE, NEVER GIVE YOUR SOCIAL SECURITY NUMBER. IF THEY HAVE YOUR INSURANCE CARD THAT'S ALL THEY NEED. IF THEY DEMAND THE SOCIAL SECURITY NUMBER LEAVE AND FIND ANOTHER DOCTOR.

USE A RECOGNIZED ANTIVIRUS SOFTWARE ON ALL COMPUTERS.

CONTACT YOUR BANK AND PUT A STRONG PASSWORD ON YOUR ACCOUNTS AND MAKE SURE IT CANNOT BE CHANGED WITHOUT YOUR CONCENT. PROVIDE AN UPDATED EMERGENCY CONTACT NUMBER FOR THE BANK TO CONTACT YOU IF ANY ACTIVITY OCCURRS ON YOUR ACCOUNT INCLUDING ADDRESS AND TELEPHONE NUMBER CHANGES.

SHRED ALL CREDIT CARD AND PERSONAL INFORMATION.

NEVER PUT MAIL OUT AND LEAVE UNATTENDED. USE THE LOCAL POST OFFICE.

GO PAPERLESS TO AVOID PERSONAL AND ACCOUNT INFORMATION BEING SENT IN THE MAIL.

IF SOMEONE CALLS YOU THAT YOU DON'T KNOW OR RECOGNIZE, HANG-UP, "DON'T TALK TO STRANGERS".

THE IRS WILL NEVER CALL AND DEMAND PAYMENT OVER THE TELEPHONE OR ADVISE YOU THEY ARE GOING TO ARREST YOU IF YOU DON'T PAY.

POP UPS ON COMPUTER TELLING YOU TO CALL A NUMBER TO CLEAR A CRASH IS A "FISHING" SCHEME WHERE THEY WANT YOUR CREDIT CARD TO CLEAR THE VIRUS. THEY WANT TO ACCESS YOUR CREDIT CARD.

WE NEED BUSINESSES AND THE GENERAL PUBLIC TO COOPERATE WITH LAW ENFORCEMENT WHEN THEY ARE INVESTIGATING FRAUD AND IDENTITY THEFT.

CONTACT YOUR TELEPHONE PROVIDER AND MAKE SURE YOU HAVE A STRONG PASSWORD ON CALL FORWARDING THAT CANNOT BE CHANGED WITHOUT FIRST CONTACTING YOU AT AN UPDATED TELEPHONE NUMBER THEY CAN MAINTAIN ON YOUR ACCOUNT.