ONLINE RESOURCES:

Consumer Financial Protection Bureau
www.consumerfinance.gov

Federal Communications Commission
www.fcc.gov/general/frauds-scams-and-alerts-guides

Internal Revenue Service
www.irs.gov/newsroom/tax-scams-consumer-alerts

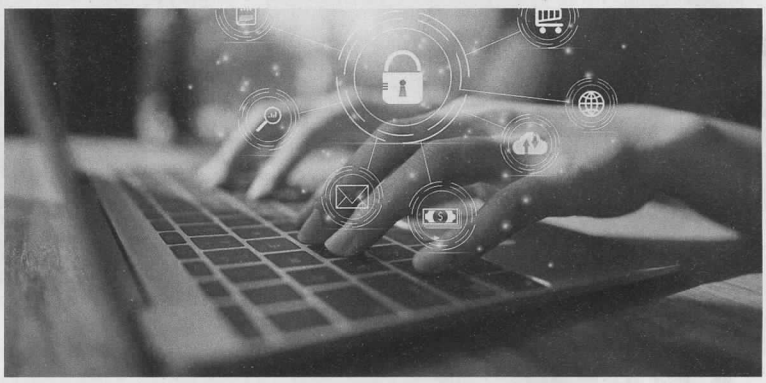
>> **FRAUD** *continued from page 82*

vanced they can create webpages mimicking banks, government agencies, etc., that look real.

- No one is coming to arrest you, garnish your money, or threaten you. That is not how real organizations work.

Prevent trouble

- Create complex passwords and change them regularly.
- Go directly to the source. If you are wondering whether a contact is real, initiate the contact by using a reliable source to contact the person or institution in question. Do not use the contact information given to you by the person talking or emailing you.
- Use credit cards instead of debit cards. Credit cards are not direct routes to your money like debit cards are. They have protections and limitations.
- Set alerts on all your accounts to warn you when a transaction takes place. Use checks sparingly. A stolen check is direct access to your cash.
- Ensure you are using the correct website and that the site is secure with "https" or the locked padlock symbol in the address.
- Have the best security protection on your computer and keep it updated.
- Shred papers and mail before you trash them. Protect your incoming mail from theft.
- Take advantage of financial readiness program services through the family center on the military installation nearest you.
- If you are serving on active duty, you can place an additional "active duty alert" on your credit report that provides protection for servicemembers for up to 12 months at a time. With this alert, creditors must take reasonable steps to ensure someone trying to open an account in your name is actually you.



Is that a real person or organization emailing you? Check with a reliable source rather than using the contact information the emailer gave you.

If you're a victim

- Change your passwords pronto. The crooks will change them to keep you from accessing your own accounts.
- Report the incident immediately to get records established indicating a crime was committed.
- Report cases of suspected identity theft to the police in order to start a record of the incident. This will come in handy down the line when it becomes difficult to distinguish between you and the scammers.
- Call all your financial institutions. Cancel credit cards. Stop transactions on accounts. The crooks will charge on your credit cards, but these have limits and protections.
- Contact Social Security to inform them.
- Call your health/Medicare program and insurance companies. Once personal information is stolen, any of your accounts can be tapped and used against you.
- Contact the Department of Motor Vehicles. Your driver's license will be modified by the crooks and used as their own ID.
- Inform the credit reporting agencies: Experian, Trans Union, and Equifax.
- Contact the business you suspect was the leak behind the theft.
- Call the IRS Identity Protection Specialized Unit at (800) 908-4490 and the Federal Trade Commission's Consumer Response Center at (877) 382-4357.
- Tell all your friends and family since your information will be used to get to them.

— By Lt. Col. Shane Ostrom, USAF (Ret), CFP®, a benefits information expert at MOAA

PHOTO: ANAWAT SUDCHANHAM/EYEEM/GETTY IMAGES