

Is your identity safe online?

INTERNET SECURITY TIPS

For Residents of the
25th Congressional District of Florida

A SERVICE OF CONGRESSMAN

Mario Diaz-Balart



Facts About Identity Theft

- Identity Theft occurs when someone steals your personal information and uses it fraudulently.
- Identity Theft can destroy your good credit and cost you a great deal of money.
- Identity Theft can take months to detect and years to fix.
- In recent years, the Internet has become a popular venue for thieves to scam innocent people.
- Once thieves possess your personal information, they can commit fraud in many different ways—with credit card accounts, bank accounts, government documents/benefits applications, employment, phone/utilities services, etc.
- The Federal Trade Commission estimates that **up to 10 million Americans** are victims of identity theft each year.
- According to the latest statistics from the FTC, **Florida is ranked #6** among states in the number of identity theft victims per 100,000 people.

Protecting Against Identity Theft

- NEVER give out personal/financial information online (including your social security number, account numbers, passwords, PINs) unless you are on a SECURE website. Secure websites have a lock icon in the bottom right corner and their web addresses begin with “https.”
- Do not open unfamiliar emails. Delete them immediately.
- Never click on links for websites sent in unsolicited/unknown emails or in pop-up windows. Physically type out the website's address yourself or locate it with a search engine.
- Use passwords that are not obvious to other people.
- Always log-out of accounts and close out windows when finished using a computer.
- Use anti-virus and anti-spyware software programs and update them often.
- Monitor your bank accounts and credit card activity regularly.
- Monitor your credit report and credit score. You are entitled to a **free** credit report annually—all you have to do is ask for it. The website **www.AnnualCreditReport.com** is a website created by the three major consumer reporting agencies (Equifax, Experian, and TransUnion) where you can order your credit report **free of charge**.
- Keep in mind that you will NEVER be asked for account information or verification via email from a legitimate company. Any email like this is fraudulent. When in doubt, call your bank or financial institution.

Common Online Scams

- Phishing is the practice of sending forged emails that pretend to be from a company you trust and have a relationship with. They ask you to verify personal or account information. They often contain a link that connects you to a website, which appears to be the legitimate company's website. This is a phony site, and allows thieves to collect the personal information they are looking for. This is called spoofing.
- Receiving an email or pop-up notification that claims that you have won a contest and are entitled to a prize, free gift, or discount. You are required to enter personal information in order to obtain the prize.
- Receiving an email from a random person asking for assistance in a money transfer to help a person in need. A cashier's check is requested from you in a large sum.
- Receiving an email from a random person informing you that you are entitled to a large monetary sum, due to the death of a distant relative or dignitary. Personal/financial information is requested in order to process the inheritance.

There are many other scams out there. These are only a few of the most commonly used ones.



If You Suspect Identity Theft

If you suspect that your identity has been compromised in any way, take the following steps IMMEDIATELY. These steps can stop thieves in their tracks, help track down the culprit, and save you time and money.

- Place a “fraud alert” on your credit reports. You can do this by contacting one of the three national consumer reporting companies—Equifax, Experian, or TransUnion. The alert tells creditors that extra precautions should be taken before allowing new accounts to be opened. The alert also entitles you to receive free copies of your credit reports. Review these for questionable inquiries or accounts.
 - > Equifax 1-800-525-6285
 - > Experian 1-888-EXPERIAN
 - > TransUnion 1-800-680-7289
- Contact the banks and financial institutions of any accounts that appear to have been opened fraudulently. Close the accounts immediately. If you suspect any of the accounts that you personally established have also been tampered with, close these as well.
- File a police report to document the criminal activity of the thieves.
- File a complaint with the Federal Trade Commission. You can do this online at **[ftc.gov/idtheft](https://www.ftc.gov/idtheft)** or by calling 1-877-ID-THEFT.



CONGRESSMAN
Mario Diaz-Balart

CONTACT INFORMATION

WASHINGTON, D.C. OFFICE

328 Cannon House Office Building
Washington, DC 20515
Telephone: (202) 225-2778
Fax: (202) 226-0346

MIAMI OFFICE

12851 SW 42nd Street
Suite 131
Miami, FL 33175
Telephone: (305) 225-6866
Fax: (305) 225-7432

COLLIER COUNTY OFFICE

4715 Golden Gate Parkway
Suite 1
Naples, FL 34116
Telephone: (239) 348-1620
Fax: (239) 348-3569

WEBSITE

www.house.gov/mariodiaz-balart

