



Karl A. Racine
D.C. Attorney General

Office of the Attorney General Consumer Alert — Privacy and Data Protection

All too often, we learn that retailers, banks, or medical professionals experience a “data breach” that compromises our personal information. You may have received a letter notifying you that your Social Security number, credit card account number, or date of birth has been stolen by a hacker.

Unfortunately, consumers who have had their sensitive information stolen are at greater risk of identity theft, fraud and other scams like email “phishing”, where a scammer poses as a trusted sender. You can protect your online privacy and personal information by practicing safe Internet habits and recognizing situations where you may expose your personal information to scammers. If you do experience identity theft, there are steps you can take to minimize any harm to your credit and reputation.

What are some of the online scams I need to be aware of?

Online auction fraud accounts for three-quarters of all complaints registered with the FBI's Internet Crime Complaint Center. There are different types of online auction fraud, but far and away the most common is paying for goods that you never receive. Beware of offers that seem too good to be true – they probably are.

You receive an e-mail that looks like it came from your bank, warning you about identity theft and asking that you log in and verify your account information. This is likely a “phishing” scam, where a scammer masquerades as a trusted sender requesting verification of your personal information, such as a Social Security number, password, or PIN. These emails are fraudulent, as legitimate businesses will not request such information via email. Successful phishers can use your information to access your accounts or impersonate you online, which can result in substantial damage to your credit and financial loss.

“IRS” scams are becoming more common, particularly among persons who file their tax returns electronically. You may receive an email that appears to be from the IRS asking you to “update your IRS e-file” and click on a link in the email. Or, your accountant may receive an email asking him to update his electronic filing information for his clients. These scams are designed to obtain e-filers’ user names, passwords, and identifying information so thieves can file false returns and steal your tax refund.

The “Nigerian” letter involves someone impersonating a foreign national who needs your help transferring money and they will pay you a fee. Delete these emails because responding could lead to the draining of your bank account and the theft of your personal information.



Connect with the Office of the Attorney General

441 4th Street, NW., Washington, DC 20001

Phone: (202) 727-3400 Fax: (202) 347-8922 TTY: (202) 727-3400

Email: Consumer.Protection@dc.gov

CONSUMER HOTLINE — (202) 442-9828

STAY CONNECTED:



www.oag.dc.gov

How do I avoid exposing my sensitive and private information online?

- ◆ Use only “secure” sites to shop or when providing information about yourself. These sites have a “lock” icon in the status bar and their address (or URL) begins with “https.”
- ◆ Don’t click on links embedded in emails or on sites to which you are transferred unless you are familiar with the sender or the website.
- ◆ Beware of unsolicited emails in which the sender asks you to provide personal information, such as a Social Security number or account number, or asks you to click on a link or open an attachment. Do not provide this kind of information, or addresses or phone numbers, including on social networking sites, and be wary of clicking on links that you do not recognize.
- ◆ Use “long and strong” passwords on online sites: Use capital and lower case letters, numbers and special characters to create passwords that are at least 8 to 10 characters long. Do not use passwords that contain your or a family member’s name, birthday, or address. Do not use the same password for multiple sites. Finally, you should change your passwords regularly.
- ◆ Assume that anyone can see your information, photos, or data if you are using a public wireless network. Make sure that your home wireless networks are password protected, or better yet encrypted, to prevent unauthorized access.
- ◆ Use security and anti-virus software programs on all your computers and devices, such as smartphones and tablets, and update that software when prompted. Updated software versions often contain security patches that help protect against malware (software programs designed to steal your personal information from otherwise secure sites).
- ◆ Recognize that photos, videos, text messages and other data stored on a computer or a phone may be backed up elsewhere, on what's commonly known as the "cloud." You should read your service provider's privacy policies to ensure the provider is agreeing to take reasonable security measures to maintain the privacy of information in the cloud.
- ◆ Be wary of “free” games and software offered on the Internet. “Free” often means that you are giving up personal information in exchange for using the product.

How do I know if my identity has been compromised?

- ◆ You may receive written notice of a data breach, which is required if you are a DC resident and your sensitive personal information is compromised. The notification should identify the kind of information that was compromised, such as names, addresses, credit or debit card information, Social Security numbers, email addresses, or passwords. If the breach involved more than 1,000 DC residents, District law requires that the breach be reported to national consumer reporting agencies.
- ◆ You may receive a fraud alert from your credit card company, or see suspicious activity on a credit card or bank statement or find withdrawals on a bank statement you do not recall making.
- ◆ You may receive unexpected bills or collection calls for goods or services you never purchased.
- ◆ You are denied credit because of negative information on your credit report that is inaccurate – *e.g.*, an unpaid debt you did not incur or you never received the bill.



Connect with the Office of the Attorney General

441 4th Street, NW., Washington, DC 20001

Phone: (202) 727-3400 Fax: (202) 347-8922 TTY: (202) 727-3400

Email: Consumer.Protection@dc.gov

CONSUMER HOTLINE — (202) 442-9828

STAY CONNECTED:



www.oag.dc.gov

What should I do if I learn my personal information has been compromised?

If you know that fraudulent activity and identify theft have occurred:

- ◆ Cancel any credit card or financial accounts you believe have been compromised or have been opened fraudulently. Consumers who timely report fraud are only liable for a maximum of \$50 in credit card charges.
- ◆ Consider placing a security freeze on your credit bureau reports with the three national credit bureaus: Equifax, Experian or TransUnion. The security freeze completely “freezes” any credit, loans or services from being approved in your name without additional consent. If you are a victim of identity theft, District law provides that you can obtain a security freeze without charge and any further freeze charges cannot be more than \$10.
- ◆ Consider researching and looking into credit monitoring services that give you regular updates on new credit accounts or suspect changes.
- ◆ Obtain a free credit report from each of the major credit bureaus. Requests for a free report based on a fraud claim can be made online at www.annualcreditreport.com or calling (877) 322-8228 or can be made directly to the credit bureaus:

TransUnion P.O. Box 6790 Fullerton, CA 92834-6790 (800) 680-7289 transunion.com	Experian P.O. Box 9532 Allen, TX 75013 (888) 397-3742 experian.com	Equifax P.O. Box 740241 Atlanta, GA 30374-0241 (800) 525-6285 equifax.com
--	---	--

- ◆ File a police report with the DC Metro Police Department and get a copy of the report as soon as it is available.

It always benefits you to diligently monitor your personal information.

Be vigilant about reviewing your financial documents. Look carefully at bank and credit card statements and report unauthorized activity or unfamiliar transactions to the bank or card company.

Periodically monitor credit bureau reports for any unusual activity and check for accuracy. Everyone is allowed one free credit report per year from each of the three major credit bureaus.

What should I do if I'm the victim of a telemarketing scam?

You can file a complaint with the District of Columbia Attorney General's Office of Consumer Protection by calling our hotline at (202) 442-9828, email (consumer.protection@dc.gov), or by writing to the **Office of Consumer Protection** at the Office of the Attorney General.

You may also file a complaint with the Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, D.C. 20580; (877) 832-4357; www.ftc.gov.



Connect with the Office of the Attorney General

441 4th Street, NW., Washington, DC 20001

Phone: (202) 727-3400 Fax: (202) 347-8922 TTY: (202) 727-3400

Email: Consumer.Protection@dc.gov

CONSUMER HOTLINE — (202) 442-9828

STAY CONNECTED:



www.oag.dc.gov