Electronic Banking (eBanking) Fraud Prevention Best Practices

v.20180319

Summary

This Document provides **consumer** and **business** Electronic Banking (eBanking) users with fraud prevention best practices.

User ID and Password Guidelines

- Create a "strong" password with at least eight characters that includes a combination of mixed case letters, numbers, and special characters. Consider using a Passphrase instead of a single word.
- Change your password frequently.
- Never share user name and password information with third-parties.
- Avoid using an automatic login feature that saves user name and passwords.

General Guidelines

- Do not use public or other unsecured computers for logging into eBanking.
- Check the last login date / time every time you log in.
- If the system does not recognize your computer or location, you will be asked to provide additional information to log into eBanking. This is called Out-of-Band Authentication via phone or SMS text.
- Review account balances and detail transactions regularly (preferably daily). Confirm payment and other transaction data, immediately report any suspicious transactions to the Bank.
- Whenever possible, use Bill Pay instead of checks to limit account number exposure and to obtain better electronic record keeping.
- Take advantage of and regularly view system alerts; examples include:

Balance alerts	Password change alerts
Transfer alerts	ACH alerts, wire alerts, or bill payment alerts

- Do not use account numbers, your social security number, or other account or personal information when creating account nicknames or other titles.
- Use the historical reporting features of your online banking application on a regular basis to confirm payment and other transaction data.
- Never leave a computer unattended while using eBanking.
- Never conduct banking transactions while multiple browsers are open on your computer.
- An FBI recommended best practice is to suggest that company users dedicate a PC solely for financial transactions (e.g., no web browsing, emails, or social media).

Electronic Banking (eBanking) Fraud Prevention Best Practices (continued)

v.20180319

Tips to Avoid Phishing, Spyware and Malware

- Do not open e-mail from unknown sources. Be suspicious of e-mails purporting to be from a financial institution, government department, or other agency requesting account information, account verification, or banking access credentials such as user names, passwords, PIN codes, and similar information. Opening file attachments or clicking on web links in suspicious e-mails could expose your system to malicious code that could hijack your computer.
- Never respond to a suspicious e-mail or click on any hyperlink embedded in a suspicious e-mail. Call the purported source if you are unsure who sent an e-mail.
- If an e-mail claiming to be from your financial organization seems suspicious, check with your financial organization.
- Install anti-virus and spyware detection software on all computer systems. Free software may not provide protection against the latest threats compared with an industry standard product.
- Update all of your computers regularly with the latest versions and patches of both anti-virus and anti-spyware software.
- Ensure computers are patched regularly, particularly operating systems, browsers, and key applications.
- Install a dedicated, actively managed firewall, especially if using a broadband or dedicated connection to the Internet, such as DSL or cable. A firewall limits the potential for unauthorized access to your network and computers.
- Check your settings and select, at least, a medium level of security for your browsers.
- Clear the browser cache before starting any eBanking session to eliminate copies of web pages that have been stored on the hard drive. How the cache is cleared depends on the browser and version you are using. This function is generally found in the browser's preferences menu.
- Be advised that you will never be presented with a maintenance page after entering login credentials. Legitimate maintenance pages are displayed when first reaching the URL and before entering login credentials.
- eBanking does not use pop-up windows to display login messages or errors. They are displayed directly on the login screen.
- eBanking never displays pop-up messages indicating that you cannot use your current browser.
- eBanking error messages never include an amount of time to wait before trying to login again.
- Be advised that repeatedly being asked to enter your password/token code are signs of potentially harmful activity.

Tips for Wireless Network Management

Wireless networks can provide an unintended open door to your business network. Unless a valid business reason exists for wireless network use, it is recommended that all wireless networks be disabled. If a wireless network is to be used for legitimate business purposes, it is recommended that wireless networks be secured as follows:

- Change the wireless network hardware (router/access point) administrative password from the factory default to a complex password. Save the password in a secure location as it will be needed to make future changes to the device.
- Disable remote administration of the wireless network hardware (router/access point).
- If possible, disable broadcasting the network SSID.
- If your device offers WPA encryption, secure your wireless network by enabling WPA encryption of the wireless network. If your device does not support WPA encryption, enable WEP encryption.
- If only known computers will access the wireless network, consider enabling MAC filtering on the network hardware. Every computer network card is assigned a unique MAC address. MAC filtering will only allow computers with permitted MAC addresses access to the wireless network.

Avoiding tech support scams

July 16, 2018
by Carol Kando-Pineda
Attorney, Division of Consumer and Business Education

You're working on your computer when, suddenly, a message pops up on the screen: "Virus detected! Call now for a free security scan and to repair your device." That's a tech support scam. Don't call, text, or email. Legit tech support companies don't operate that way.

Scammers pose as big-name companies and use pop-up messages, fake websites, and phone calls to trick you into thinking your computer has an urgent problem. Their plan is to get your money by selling you worthless software, enrolling you in fake programs, or getting you to pay for useless tech support. The scammers urge you to call a toll-free number immediately, threatening that you may lose personal data if you don't.

When you call, the scammer might ask you to give them remote access, pretend to run a diagnostic test, or tell you they've found a virus or other security issue. They try to sell you a security subscription or other "services" that range from worthless (for instance, they're available for free elsewhere) to malicious (they install dangerous software that can help them steal your personal information.)

What should you do? If you get a pop-up to call a number to fix a virus on your computer, ignore it. Your computer is almost certainly fine. But if you're concerned about your computer, call your security software company directly — and don't use the phone number in the pop-up or on caller ID. Use a number you know is real, like the one on a software package or your receipt. Tech support scammers like to place online ads pretending to be legitimate companies, so be sure you have the correct telephone number for the real tech company before calling.

And if someone asks you to pay for anything — including tech support services — with a gift card, cash reload card, or a wire transfer, that's a scam. No legitimate company will tell you to pay that way. If you see that, report it at FTC.gov/complaint.

Source: www.consumer.ftc.gov/blog

Online love asking for money? It’s a scam.

July 10, 2018
by Carol Kando-Pineda Attorney, Division of Consumer and Business Education

While plenty of successful relationships begin online, scammers also use online dating sites, apps, and chat rooms to trick you into sending them money. These imposters create fake profiles to build online relationships, and eventually convince people to send money in the name of love. Some even make wedding plans before disappearing with the money. It’s a big problem: reports to the FBI about online romance scams tripled between 2012 and 2016, and imposter scams were among the top reports to the Federal Trade Commission for both the general population and the military community.

These scams can take a military angle with imposters stealing servicemembers’ photos to create phony profiles. They might claim to be servicemembers who can’t get into their accounts overseas or who need money fast. The first sign of a scam is an online love interest who asks for money. But the Army’s Criminal Investigative Service (CIS) says that the military doesn’t charge servicemembers to go on leave, get married, communicate with their family, go online, or feed and house themselves on deployment. We have also heard of scammers re-using servicemembers’ photos again and again, so it can be helpful to do some online research on the love interest’s name, photos, and details to check the story out.

If an online love interest asks you for money:

- Slow down and talk to someone you trust. These scammers want to rush you, often professing love right away; or pressuring you to move your conversation off the dating site.
- Never wire money, put money on a gift card or cash reload card, or send cash to an online love interest. You won’t get it back.
- If you sent money to a scammer, contact the company you used to send the money (wire transfer service, gift card company, or cash reload card company) and tell them it was a fraudulent transaction. Ask to have the transaction reversed if possible.
- Report your experience to the dating site and to the FTC.

Source:www.consumer.ftc.gov/blog

Student loan debt relief customers: Take 2 steps

July 3, 2018

by Lesley Fair Attorney, Division of Consumer and Business Education, FTC

Do you have student loans? Did you respond to an ad from Ameritech Financial claiming to offer you debt relief? The FTC has sued Ameritech for deceptive practices and just sent letters about the case to thousands of customers. The court hasn't ruled, but there are steps you can take now to make sure your payments are going toward your loans. In addition, Ameritech may have changed your Federal Student Aid (FSA) account information. There are steps you can take to protect your financial privacy.

Here are answers to questions consumers are asking.

How do I know if Ameritech Financial is the company I do business with?

In addition to the name Ameritech, the company uses the names American Financial Benefits Center, AFB, AF Student Services, and Financial Education Benefits Center (FEBC).

I'm making monthly payments to Ameritech. Are those payments going toward my student loans?

No. Your monthly payments to Ameritech **do not** go toward paying your student loans. And Ameritech **does not** make payments on your behalf to your loan servicer.

Why is the FTC suing Ameritech?

According to the FTC, Ameritech failed to deliver on its promise that people could permanently reduce their monthly payments or get total loan forgiveness. The FTC also says the company charged illegal upfront fees. In addition, the FTC alleges the company told people their fees would go toward their student loan balances, but that wasn't true.

Do I need to pay Ameritech to take advantage of loan repayment or forgiveness programs?

No. The Department of Education doesn't charge borrowers to enroll in repayment and forgiveness programs. That means you are currently paying Ameritech for things you can get for free on your own from the Department of Education.

Can I stop making monthly payments to Ameritech?

Yes. To cancel your membership, call Ameritech at 1-800-792-8621. Canceling will not impact your student loans.

Will I get my money back?

The FTC works to return as much money as possible to consumers. But this case is still in court, so there's no way to know if it will result in refunds. Legal actions take time, so please be patient. As soon as we have updates, we'll post them here.

How can I tell the FTC about my experience with Ameritech?

File a report at FTC.gov/complaint. Your information will go into a secure database the FTC and other law enforcement agencies use for investigations. When you go to FTC.gov/complaint, click on: Credit and Debt, then Debt, and then A company offering debt management or credit counseling.

What can I do to protect my financial privacy?

Ameritech may have changed your Federal Student Aid (FSA) account information. So you may want to change your login and review your account. Call Ameritech at 1-800-792-8621 or contact your loan servicer to regain control of your account.

How can I check the status of my loans and the security of my account?

Contact your loan servicer.

I've seen other companies claim they can reduce my student loan debt. How can I protect myself from questionable practices?

Visit www.ftc.gov/studentloans. One tip: It's illegal for companies to ask for money up front for so-called debt relief services. Don't do business with anyone who makes you pay before getting the results they promise.

Source:www.consumer.ftc.gov/blog

Getting a vacation rental? Watch out for scams.

July 2, 2018
By Ari Lazarus Consumer Education Specialist, FTC

With July 4th right around the corner, plenty of us are still running around trying to book a last-minute vacation rental. If that's you, here's what you need to know: scammers are ready with fake vacation rental ads. Rental scammers try to get your rental booking and take your money. But, when you show up for the vacation, you have no place to stay and your money is gone!

Here are some of the ways they pull off the scam:

Some scammers start with real rental listings. Then they take off the owner's contact information, put in their own, and place the new listing on a different site — though they might continue to use the name of the actual owner. In other cases, scammers hijack the email accounts of property owners on reputable vacation rental websites.

Other scammers don't bother with real rentals — they make up listings for places that aren't really for rent or don't exist. To get people to act fast, they often ask for lower than average rent or promise great amenities. Their goal is to get your money before you find out the truth.

So how do you avoid a rental scam?

- **Don't wire money or pay with a prepaid or gift card for a vacation rental.** Once the scammer collects the money, it is almost impossible to get it back.
- **Don't be rushed into a decision.** If you receive an email pressuring you to make a decision on the spot for a rental, ignore it and move on.
- **Look out for super cheap rates for premium vacation properties.** Below-market rent can be a sign of a scam. Do some extra research to confirm the deal is legitimate before jumping in.
- **Get a copy of the contract before you send any deposit money**. Check that the address of the property really exists. If the property is located in a resort, call the front desk and confirm the location of the property and other details on the contract.

If you come across any of these ads, we want to hear about it — report it to us at ftc.gov/complaint, whether you lost money or not.

If you sent money to a rental scammer, contact the company you used to send the money, such as your bank, Western Union, MoneyGram, Green Dot, iTunes, or Amazon and tell them the transaction was fraudulent. They may not be able to get your money back, but it is important to alert them of fraud.

Source:www.consumer.ftc.gov/blog

Watch out for these new tax scams

March 12, 2018
by Colleen Tressler
Consumer Education Specialist, FTC

They're at it again... tax scammers scheming new ways to steal personal information and money.

In the first scenario, identity thieves file a fake tax return and have the refund deposited into your bank account. The thieves then contact you, often by phone, and — posing as the IRS or debt collectors for the IRS — demand you return the money to the IRS. But following the thieves' instructions actually sends the money to them.

In another version, after you get that erroneous refund, you get an automated call, allegedly from the IRS, threatening you with criminal fraud charges, an arrest warrant, and "blacklisting" of your Social Security number. The caller gives you a case number and a telephone number to call to return the refund.

Don't take the bait. If you or someone you know gets an unexpected tax refund, follow the guidance outlined by the IRS for how to return the funds to the agency. The steps for returning paper checks and direct deposits differ.

In a different scam, criminals are using imposter tax preparation sites and phone numbers to steal peoples' personal information. Here's how this scam works: You go online to find a tax preparation service to prepare and e-file your tax return. But instead of landing on a legitimate site, you mis-click to a look-alike site created by scammers. The site looks real, and it's set up to collect personal information that can be used to commit fraud, including identity theft.

The FTC has these tips to fight tax identity theft:

- File your tax return early in the tax season, if you can.
- Use a secure internet connection if you file electronically, or mail your tax return directly from the post office.
- When using an online tax preparation service, look for the tax preparer identification number. The IRS requires all paid tax preparers to have one before filing any returns.
- To determine if a website is encrypted, look for https at the start of the web address (the "s" is for secure). Some websites use encryption only on the sign-in page, but if any part of your session isn't encrypted, your entire account could be vulnerable. Look for https on every page you visit, not just when you sign in.
- Ask tax preparers about their data security policies, and how they protect your information.
- Respond to all mail from the IRS as soon as possible.
- If tax identity theft happens to you, visit IdentityTheft.gov to report it to the FTC, file an Identity Theft Affidavit with the IRS electronically, and get a personal recovery plan.

Has an online love interest asked you for money?

February 1, 2018
Colleen Tressler
Consumer Education Specialist, FTC

Looking to start a new relationship? For some, that may mean meeting a new love interest online. Word to the wise: sometimes it's best to lead with your head and not your heart.

Millions of Americans use dating sites, social networking sites, and chat rooms to meet people. And many forge successful relationships. But scammers also use these sites to meet potential victims. They create fake profiles to build online relationships, and eventually convince people to send money in the name of love.

The Federal Trade Commission receives thousands of reports each year about romance scammers who create fake online relationships only to steal their victims' money.

Unfortunately, an online love interest who asks for money is almost certainly a scam artist.

The FTC's new infographic, developed with the American Bankers Association Foundation, lists common signs of online dating scams and what to do if someone you meet online asks you for money.

Below are some tips to identify a real romance versus a scammer cruising for a target.

- Has an online love interest asked you for money? That's a scam
- Scammers know millions of people use online dating sites. They are there, too, hiding behind fake profiles.
- Signs of a scam:
    - Professes love quickly
    - Claims to be from the U.S., but is overseas for business or military service
    - Asks for money, and lures you off the dating site.
    - Claims to need money – for emergencies, hospital bills, or travel
    - Plan to visit, but can't because of an emergency

Please share this information with others. Victims may be embarrassed to talk about their experiences, but you can help. A simple phone call, email or text, saying "Look what I just found" and sharing this information may make a difference in someone else's life**.**

U.S. Marshals won’t call you about jury duty

December 6, 2017
Bridget Small
Consumer Education Specialist, FTC

United States Marshals protect the federal courts, track down dangerous fugitives, and transport thousands of prisoners. They don’t make calls and threaten to arrest people or fine them for missing jury duty. But scammers posing as Marshals have been making calls like that and tricking people into sending money. The imposters use spoofed phone numbers that look official, and steal the names and badge numbers of legitimate law enforcement officials. They warn people they might be arrested — unless they buy a prepaid debit, iTunes or gift card and pay the fine immediately. If you buy a card and tell a scammer the card’s code, the scammer takes the card’s value; your money is gone. If a “U.S. Marshal” calls you with a jury duty warning, hang up. It’s a scam.

If a fake Marshal — or any other government imposter — calls and tells you to send money to avoid arrest:

- Don’t send money by prepaid card and don’t wire money. Wiring money is like sending cash. You usually can't reverse or trace the transaction.
- Don’t share your financial or personal information. Scammers can use your information to commit identity theft.
- Don’t trust a name or number that appears on your phone. Scammers can fake caller ID information.

If you received a call like this, please report it to the FTC and to your local Marshals Service District Office. If you sent money to an imposter on a prepaid card, report it to the card company’s fraud department. Read more about the tricks government imposters use and how to beat their scams.

No secret bank accounts to pay your bills

August 17, 2017
By Colleen Tressler
Consumer Education Specialist, FTC

Another day, another scam. Case in point: the Federal Reserve Bank of New York reports that scammers are telling people they can pay their bills using so-called “secret accounts” or “Social Security trust accounts” and routing numbers at Federal Reserve Banks. In exchange for personal information, like Social Security numbers, people get what they think is a bank account number at a Federal Reserve Bank. But this really is just a way to get your personal information, which scammers can then sell or use to commit fraud, like identity theft.

It’s good to keep in mind that people do not have accounts at Federal Reserve Banks. Only *banks* can bank at the Federal Reserve. But what happens if you try to use this “secret” account? Well, the Federal Reserve Bank will deny the payment, since you don’t really have an account there. Once the payment is rejected, you’ll be notified that you still owe the money – which is about when you might figure out that this was a scam. At that point, you may owe a late fee or penalty to the company you thought you were paying. You also may owe fees to your bank for returned or rejected payments.

If you see a video, text, email, phone call, flyer, or website that describes how you can pay bills using a Federal Reserve Bank routing number or account, report it to the FTC. It’s a scam. And remember: never give your credit card, bank account, or Social Security number to anyone who calls or emails and asks for it – no matter who they say they are.

Payments you didn’t authorize could be a scam

August 16, 2017
By Rosario Méndez
Attorney, Division of Consumer & Business Education, FTC

Usually, when I pay with a check, I write it out and sign it, or I direct my bank to send it on my behalf. But what if a check is drawn on my account but I didn’t write it, sign it, or tell my bank to send it? It can happen if someone has your bank account number: they can use your number to create a check that takes money out of your account. Now, if you’d already agreed to the charges, there’s no problem. But what if you didn’t? That means this check is part of a scam – which is what the FTC says happened in a case announced today.

The FTC sued several companies and individuals for allegedly taking millions of dollars out of people’s accounts using remotely created checks – without the account owners’ authorization. The defendants had websites and made telemarketing calls that offered short-term loans and cash advances to people with bad credit. To get access to that money, people gave their bank account information. But the FTC says the defendants actually signed people up for online discount membership clubs – and charged for them. People had not agreed to that, and it only made their situations worse. When people complained to the company, the FTC says the defendants lied to confuse people into thinking they had, in fact, approved those charges.

Here are three things you can do to outsmart scammers.

1. **Stop before you put your account information in a website**. Ask yourself: who, exactly, am I dealing with? Can I trust them? What will they do with my information? Dishonest people may use your bank or credit card information to take your money, or sell your information to others who’ll do the same.

2. **Review your bank account and credit card statements carefully.** Check for charges you don’t recognize, remember agreeing to, or that you didn’t authorize – especially if you recently applied for a loan or credit.

3. **Tell your bank or credit card company immediately** if you see a check or charge you don’t recognize. If the unauthorized charge is part of a scam, telling your bank and the FTC might help stop the scammers.

“I have an emergency and need money”

April 13, 2017

by Jennifer Leach
Assistant Director, Division of Consumer and Business Education

If you’ve ever gotten one of those calls, you know how alarming they can be. And that’s exactly what the scammers count on. They want you to act before you think – and acting always includes sending them money: by wiring it or by getting a prepaid card or gift card, and giving them the numbers on the card. Either way, your money’s gone.

Here’s the story of Pablo Colón from Bridgeport, Connecticut, and his family. When both his sister and his father got a call about a family “emergency,” Pablo spotted the scam. And, luckily for the good people of Bridgeport, Pablo’s family owns a radio station – so he put the story on the air and warned his community.

Talking about a scam is important – even if only one person is listening, instead of the thousands who heard Pablo’s story. So watch this video. And then pass it on. Today, tell someone about this scam, about Pablo’s story, about why we should all talk about the scams we see. And, whenever you spot a scam, please tell the FTC.

Don't bank on that check

March 17, 2017
by Lisa Lake
Consumer Education Specialist, FTC

Scammers know how to design phony checks to make them look legitimate. In fact, the Council of Better Business Bureaus just released a list of the most “risky” scams, based on how likely people are to be targeted, how likely to lose money, and how much money they lost. Fake checks were number two.

Fake checks drive many types of scams – like those involving phony prize wins, fake jobs, mystery shoppers, online classified ad sales, and others. In a fake check scam, someone asks you to deposit a check – sometimes for several thousand dollars – and, when the funds seem to be available, wire the money to a third party. The scammers always have a good story to explain the overpayment – they’re stuck out of the country, they need you to cover taxes or fees, you’ll need to buy supplies, or something else. But when the bank discovers you’ve deposited a bad check, the scammer already has the money, and you’re stuck paying the money back to the bank.

So don’t deposit a check and wire money or send money back in any way. Banks must make funds from deposited checks available within days, but uncovering a fake check can take them weeks. If a check you deposit bounces – even after it seemed to clear – you’re responsible for repaying the bank. Money orders and cashier’s checks can be counterfeited, too.

Want to avoid the latest rip-offs? Sign up for free scam alerts from the FTC at ftc.gov/scams.

Government imposters want to get to know you

March 9, 2017

by Lisa Lake
Consumer Education Specialist, FTC

The Office of the Inspector General (OIG) for the Department of Health and Human Services (HHS) and the FTC want you to know about a scam in which callers posing as federal employees are trying to get or verify personal information. This is a government imposter scam.

Sometimes, the caller asks you to verify your name, and then just hangs up. Other times, he or she might ask for detailed information — like the last digits of your Social Security or bank account number. Imposters might say they need this information to help you or a family member. But their real reason is to steal from you or sell your information to other crooks.

Your caller ID might even read “HHS Tips” or “Federal Government” when they call. The phone number could have the “202” Washington, DC area code, the headquarters for many federal agencies. The phone number may even be for a real government agency. But don’t be fooled: Scammers know how to rig their caller IDs to show false information.

So how can you tell the caller is an imposter?

- The federal government typically will contact you by U.S. Mail first, **not by phone or email**.
- Federal agencies **will not demand personal information** like your Social Security Number or bank account number over the phone. Also, just because the caller knows details about you, doesn’t mean she is trustworthy.
- The caller typically asks you to send money – often via wire transfer, by using a prepaid debit card, or maybe by sending you a fake check to cash. Federal agencies **will not** ask you to use *any* of these methods to send money for *any* reason.

…and what should you do?

- **Hang up**. Do not give out any personal or financial information.
- **Contact the Department of Health and Human Services OIG** at 1-800-HHS-TIPS (1-800-447-8477) or spoof@oig.hhs.gov
- **File a complaint with the FTC** at ftc.gov/complaint or 877-FTC-HELP.
- **Learn more** about government imposter scams and sign up for the FTC’s Scam Alerts.
- Pass on what you’ve learned to older consumers and others.

A government program that pays your bills?

January 24, 2017

by Sana Chriss
Attorney, Southeast Region, Federal Trade Commission

Have you heard about a government program that will pay your monthly bills for an up-front payment or processing fee? Here's a short version of the rest of this post: It's a scam. Don't do it.

We've heard that this scam is happening in some African-American church communities: people approach church-goers with this so-called deal. And, because it comes up in church, the scam might seem like it could be legit. But take it from me – and the FTC: there is **no** federal program that pays your monthly bills in exchange for payment of any kind.

What really happens if you pay these scammers? They look real for a minute because they "pay your bills" electronically – but then they cancel the payment. You think your bill is paid, but you're stuck with not only the original bill, but also a late fee because your payment wasn't actually processed. And now the scammers have your bank or credit information. Doesn't sound like much of a deal at all.

If you need help paying bills, or know someone who does, there are some legitimate government sites that can connect you with programs that help with things like medical bills and energy services for people who are eligible. But they won't ask **you** to pay **them**. Also check out how to make a budget or find a credit counselor who can help you manage your money.

IRS warns of a new tax bill scam

November 17, 2016
by Seena Gressin
Attorney, Division of Consumer & Business Education, FTC

We certainly understand if the latest IRS imposter scam makes you queasy: it involves a fake IRS tax notice that claims you owe money as a result of the Affordable Care Act.

The IRS says the fake notices are designed to look like real IRS CP2000 notices, which the agency sends if information it receives about your income doesn't match the information reported on your tax return. The IRS says many people have gotten the bogus notices, which usually claim you owe money for the previous tax year under the Affordable Care Act.

It's one of many IRS imposter scams that have popped up. As tax season nears, we'll see more. The good news? There are red-flag warnings that can help you avoid becoming a victim. For example, the IRS will never:

- Initiate contact with you by email or through social media.
- Ask you to pay using a gift card, pre-paid debit card, or wire transfer.
- Request personal or financial information by email, texts, or social media.
- Threaten to immediately have you arrested or deported for not paying.

In the new scam, the fake CP2000 notices often arrive as an attachment to an email — a red-flag — or by U.S. mail. Other telltale signs of this fraud:

- There may be a "payment" link within the email. Scam emails can link you to sites that steal your personal information, take your money, or infect your computer with malware. Don't click on the link.
- The notices request that a check be made out to "I.R.S." Real CP2000s ask taxpayers to make their checks out to "United States Treasury" if they agree they owe taxes.

In the version we saw, a payment voucher refers to letter number LTR0105C, and requests that checks be sent to the "Austin Processing Center" in Texas. But scammers are crafty. They could send messages with a variety of return addresses.

Empowering Latinos to know their rights and avoid scams

September 9, 2016
by Alvaro Puig
Consumer Education Specialist, FTC

Hispanic Heritage Month is a time to celebrate the contributions so many Latinos have made throughout history. It's also a time for us to celebrate **you** for the vital role you've played in helping Latino communities avoid scams.

In the past year, you:

- visited consumidor.ftc.gov almost 1.3 million times to do things like learn about financing a car; look into the cost of funeral services; find out how to order a free copy of your credit report; investigate if opportunities to make money working from home are legit or a scam; decide if home equity lines of credit are right for you; find out what to do if your credit or debit card is blocked; learn about your rights when a debt collector contacts you; find out what to do about illegal robocalls; and how to get a sample complaint letter to send to a company.
- took to social media to spread the word about scams like at-home medical billing and fake international driver's licenses
- signed up to get our free email updates— a whopping 10,000 of you became new subscribers
- ordered more than 1.6 million free publications in Spanish like a guide for parents about talking with kids about online safety and a booklet for kids about how to socialize online safely; an identity theft bookmark and a tip sheet that tell you what to do right away if someone is using your information; and our series of fotonovelas in Spanish with tips on how to avoid a notario scam, a government imposter scam, an income scam and a debt relief scam; how to deal with debt collectors; and how to avoid financing trouble when you buy a car.

Thank you for being an informed consumer, and for helping your community!

This Hispanic Heritage Month, and year-round, we invite you to order publications and share them. The cost of the publications and the shipping is on us! That's right, they're free.

You know where to find us, so please tell your friends they can visit us and find free tips at consumer.ftc.gov, get free email alerts, follow us on Twitter and Facebook, and watch our videos on YouTube.

Voicemail from an IRS imposter?

September 1, 2016
by Andrew Johnson
Division of Consumer and Business Education, FTC

You get a call or voicemail from someone claiming to be from the IRS. You're being sued and this your final notice. Don't panic. And don't return the call. It's a scam.

Here are a few facts about the IRS to keep in mind if you get a similar call:

- If the IRS needs to contact you, they'll do it by mail first.
- The IRS won't demand personal information like credit card or Social Security numbers over the phone.
- The IRS won't threaten to arrest or sue you, or demand that you pay right away. The IRS also won't tell you to use a specific form of payment like a money transfer from MoneyGram or Western Union, a cash reload from MoneyPak or Reloadit, or a gift card from iTunes or Amazon. Scammers ask you to use those ways to pay because they're hard to track or cancel payments.

If you or someone you know receives a call like this, report it the FTC and the Treasury Inspector General for Tax Administration (TIGTA). Include the caller's phone number, along with any details you have. If you're not sure whether a call is really from the IRS, you can double-check by calling the IRS directly at 1-800-829-1040. For more, check out this IRS imposter scams infographic. Share with friends and family. They may get the call next.

The top three ways to avoid fraud

August 26, 2016
by Jennifer Leach
Assistant Director, Division of Consumer and Business Education

In pretty much every article and blog post we put out, you'll find tips to help you avoid scams. The idea is that, if you can spot a scam, and know how to avoid it, you and your money are more likely to stay together.

Today, we're releasing a brochure that distills those tips down to the top 10 ways to avoid fraud. This brochure – available online and in print – is your one-stop resource to help you spot imposters, know what to do about robocalls, and how to check out a scammer's claims.

Here are three things that can help you avoid scammers who try to call you:

1. **Hang up on robocalls**. If you pick up the phone and hear a recorded sales pitch, hang up and report it to the FTC. These calls are illegal. And plentiful. Don't press 1, 2 or any number to get off a list or speak to a person. That just means you'll get even more calls.
2. **Don't trust your caller ID**. Scammers can make caller ID look like anyone is calling: the IRS, a business or government office…even your own phone number. If they tell you to pay money for any reason, or ask for your financial account numbers, hang up. If you think the caller might be legitimate, call back to a number you know is genuine – not the number the caller gave you.
3. **Talk to someone**. Before you give up money or information, talk to someone you trust. Scammers want you to make decisions in a hurry. Slow down, check out the story, search online – or just tell a friend. We find that people who talk to someone – anyone – are much less likely to fall for a scam.

For seven more tips to help protect yourself and loved ones from fraud, read on – or order your free copies of 10 Things You Can Do to Avoid Fraud to share in your community. And if you spot something that looks like a scam, report it to the FTC.

Unauthorized Banking: Banc of Omaha

August 25, 2016

Office of the Comptroller of the Currency

The Office of the Comptroller of the Currency (OCC) has been informed that an entity calling itself Banc of Omaha purports to be a lender specializing in business capital. Banc of Omaha is not a licensed or chartered bank but is using a logo similar to that of Mutual of Omaha Bank, which is a chartered financial institution regulated by the OCC.

Business owners and consumers (who may not be business owners) are receiving letters by fax and mail stating that their company has been approved for up to $250,000 in working capital. The letter pressures the recipient to respond by a deadline because of limited funds. The correspondence is signed by Sam Thomas and includes a telephone number of (800) 706-7712 and a website address of [www.BancofOmaha.com]. When the telephone number is dialed, an automated recording announces itself as Banc of Omaha; however, the individual who then answers the line provides the names of “Business Services” and “U.S. Business Capital.” No physical addresses are available for these entities.

Additional information concerning this matter that should be brought to the OCC’s attention may be forwarded to:

Office of the Comptroller of the Currency

Special Supervision Division

400 7th St. SW, Suite 3E-218; MS 8E-12

Washington, DC 20219

Phone: (202) 649-6450

Fax: (571) 293-4925

occalertresponses@occ.treas.gov

Scams, Too

June 24, 2016

by Lisa Lake

Consumer Education Specialist, FTC

What's worse than losing money to a scammer? Losing more money to another scammer claiming to help you recover from the first one.

Yep; this really happens. It works like this: Con artists contact you because you're on their lists of people who lost money to scams. For a "small fee" or "donation" upfront, they promise to recover the money you lost from a prize scheme, bogus product offer, or some other scam.

Sometimes, they try to get you to contact *them* by putting their offers of "help" in the comments section of blog posts or online articles about scams. Some crooks claim to be from a government agency to appear trustworthy. Others pretend to be actual victims who got (supposed) help from some (fake) agency or company.

But it's all just a scam, too — another way for a scammer to profit from your loss. They're after your money, and if you share your payment information, they've got it.

Here's how you can avoid these recovery scams:

1. **Don't pay upfront for a promise.** Someone might ask you to pay in advance for things – like help with recovering from a scam. Consider it a no-go if they ask you for money before they provide any "help".
2. **Don't send money or give out personal information** in response to an unexpected text, phone call, or email.
3. **Do online searches**. Type the name or contact information into your favorite search engine with the term "complaint" or "scam."
4. **Sign up for the FTC's free scam alerts at ftc.gov/scams** for the latest tips and advice about scams.

And if you find yourself scammed after being scammed, file a complaint with the FTC.

Learn how to fight fraud – at your library!

June 1, 2016
by Carol Kando-Pineda
Counsel, FTC's Division of Consumer & Business Education

Book lovers flock to their local library to pick up a favorite classic or the latest bestseller. But today library visitors also want and need a whole lot more. In addition to providing traditional services, librarians help diverse groups of people navigate a complicated world, including how to avoid scams.

As for scams, there's one thing we know for sure: we're all consumers – and we're all targets for fraud. Scammers are good at what they do. They're professionals who know how to create confusion and prey on emotions to throw people off-balance just long enough to take advantage. Our job is to give people a heads-up so that maybe they don't get knocked off balance and they don't get ripped off.

What does that heads-up look like? It depends on the topic and the community. The FTC wants to help librarians help all their patrons. That's why we asked legal services lawyers, librarians, ESL teachers, military counselors and others working in various communities: What kinds of scams do your folks experience? What do they need to know? What's the best way to reach them? Then we developed resources to address those needs for: people with challenges reading English, older patrons, Spanish-speakers, identity theft victims, new arrivals, and families looking to start a conversation with kids about digital literacy and living life online. Coming soon are tips and tools to address the particular consumer challenges military families face.

We've gathered these resources in one convenient spot, FTC.gov/Libraries. It's a great place to start exploring ways to fight fraud. Librarians can:

- Use the content in library programming.
- Order free copies of bookmarks and other print resources.
- Add information to your newsletters, sites, or social networks. We have about 100 videos – they make great snackable tips for your social media!

Take a look around FTC.gov/Libraries – we'd love to hear what think.