NION BANK

Mobile Banking App is HERE!



April 2024

Stop Unwanted Robocalls and Texts

Unwanted calls – including illegal and spoofed robocalls - are the FCC's top consumer complaint and our top consumer protection priority. These include complaints from consumers whose numbers are being spoofed or whose calls are being mistakenly blocked or labeled as a possible scam call by a robocall blocking app or service. The FCC is committed to doing what we can to protect you from these unwelcome situations and is cracking down on illegal calls in a variety of ways:

- Issuing hundreds of millions of dollars in enforcement actions against illegal robocallers.
- Empowering phone companies to block by default illegal or unwanted calls based on reasonable call analytics before the calls reach consumers.
- Allowing consumer options on tools to block calls from any number that doesn't appear on a customer's contact list or other "white list."
- Requiring phone companies to implement <u>caller ID authentication</u> to help reduce illegal spoofing.
- Making consumer complaint data available to enable better call blocking and labeling solutions.

Check out the consumer guide on <u>Call Blocking Tools and Resources</u>, which includes information on many of the call blocking and labeling tools currently available to consumers.

Learn more about <u>FCC Initiatives to Combat Robocalls and Spoofing</u> and download the FCC Report on Robocalls.

<u>File a complaint with the FCC</u> if you believe you have received an illegal call or text, or if you think you're the victim of a spoofing scam. Click the tabs below for tips, FAQs and resources.



Middlebourne Office 103 Dodd Street Middlebourne, WV 26149 304-758-2191

Sistersville Office 700 Wells Street Sistersville, WV 26175 304-652-3511

St. Marys Office 401 Second Street St. Mary's, WV 26170 304-684-2427

Hundred Office 3924 Hornet Hwy, Hundred WV 26575 304-775-2265

Ellenboro Office 90 Main Street Ellenboro, WV 26346 304-869-3232

Harrisville Office 1500 E. Main Street Harrisville, WV 26362 304-643-2974

Pennsboro Office 214 Masonic Ave. Pennsboro, WV 26415 304-659-2964

> Marietta-Loan Production By Appointment Only

New Martinsville Office 638 N SR 2 New Martinsville, WV 26155 304-455-2967



Consumer Tips to Stop Unwanted Robocalls and Avoid Phone Scams

- Don't answer calls from unknown numbers. If you answer such a call, hang up immediately.
- You may not be able to tell right away if an incoming call is spoofed. Be aware: Caller ID showing a "local" number does not necessarily mean it is a local caller.
- If you answer the phone and the caller or a recording - asks you to hit a button to stop getting the calls, you should just hang up. Scammers often use this trick to identify potential targets.
- Do not respond to any questions, especially those that can be answered with "Yes."
- Never give out personal information such as account numbers, Social Security numbers, mother's maiden names, passwords or other identifying information in response to unexpected calls or if you are at all suspicious.
- If you get an inquiry from someone who says they represent a company or a government

agency, hang up and call the phone number on your account statement, in the phone book, or on the company's or government agency's website to verify the authenticity of the request. You will usually get a written statement in the mail before you get a phone call from a legitimate source, particularly if the caller is asking for a payment.

- Use caution if you are being pressured for information immediately.
- If you have a voice mail account with your phone service, be sure to set a password for it. Some voicemail services are preset to allow access if you call in from your own phone number. A hacker could spoof your home phone number and gain access to your voice mail if you do not set a password.
- Talk to your phone company about call blocking tools they may have and check into apps that you can download to your mobile device to block unwanted calls.
- If you use robocall-blocking technology already, it often helps to let that company know which numbers are producing unwanted calls so they can help block those calls for you and others.

To block telemarketing calls, register your number on the <u>Do Not Call List</u>. Legitimate telemarketers consult the list to avoid calling both landline and wireless phone numbers on the list.



Sources/Credit: Article: sion, January 2024

Federal Communications Commission, January 2024
Images:

Images by <u>Peggy und Marco Lachmann-Anke</u> from Pixabay, Attribution: Pixabay, <u>Pixabay Content License Summary</u>

New Tax Scam To Watch For In 2024



The IRS is warning people about a new surge in scams affecting taxpayers this filing season. Identity thieves are targeting accounting and tax preparation groups with phishing campaigns, pretending to be prospective clients to gain access to sensitive data. These phishing emails contain malicious links that can collect the tax preparer's contact information, passwords, and even client information if clicked.

Scammers then use this information to reach out to unsuspecting clients, posing as the tax preparer in order to obtain their personal information.

How you can protect yourself

If you receive an unexpected or suspicious-looking email from an accountant or tax preparation firm, always verify the sender's identity by using another communication method. The safest method is typically looking up the company's phone number and placing a call to confirm.

How to report tax scams

Unfortunately, tax season is prime time for cybercriminals to pose as tax officials, from small preparation firms to IRS officers. Learn more about common scams and how to protect yourself with this short video.

If you suspect you've received a fraudulent message from someone purporting to be from the IRS, file a complaint with the:

- Internal Revenue Service (IRS)
- Federal Trade Commission (FTC)
- Treasury Inspector General for Tax Administration (TIGTA)

If you believe you have provided your confidential information (e.g., Social Security Number, financial records, etc.) during a phishing attempt, visit identitytheft.gov to report it to the IRS and FTC and create an action plan to begin protecting your identity.

Sources/Credit:

Articles:

Weill Cornell Medicine Information Technologies & Services, March 6, 2024

Image by Mohamed Hassan from Pixabay; Attribution: Pixabay, Pixabay Content License Summary

Tax & IRS Scams

We are in tax season again, which can be an active and lucrative time for scammers. Here is a list of scams you may encounter in this tax

'We recalculated your tax refund, and you must fill out this form.'

These scam emails display the IRS logo and use subject lines such as "Tax Refund Payment" or "Recalculation of your tax refund payment." It asks people to click a link and provide their Social Security numbers, birthdays, addresses, driver's license numbers, and other personal information to submit a fake form to allegedly claim their refund. These scammers may sometimes use a ".edu" email address to target college students.

'We're calling from the FDIC and need your bank information.'

The Federal Depository Insurance Corporation insures bank deposits so that consumers won't lose all their money if a bank fails. But it does not send unsolicited correspondence asking for money, sensitive personal information, bank account.

Information, credit and debit card numbers, Social Security numbers or passwords. Scammers claiming to be from the FDIC are hunting for information they can use to commit fraud or sell identities.

'We're calling to tell you your identity was stolen; you need to buy some gift cards to fix it.

In this trick, a criminal calls the victim and poses as an IRS agent. The criminal claims the victim's identity has been stolen and that it was used to open fake bank accounts. The caller then tells the taxpayer to buy certain gift cards; later, the crook gets back in touch and asks for the gift card access numbers.

'We'll cancel your Social Security number.'

In this IRS scam, the criminal contacts the victim and claims that they can suspend or cancel the victim's Social Security number.

"If taxpayers receive a call threatening to suspend their SSN for an unpaid tax bill, they should just hang up," the IRS says.

'This is the Bureau of Tax Enforcement, and we're putting a lien or levy on your assets.

There is no Bureau of Tax Enforcement. Victims often receive a letter from the fake agency claiming that they have a tax lien or tax levy and that they had better pay the "Bureau of Tax Enforcement" or else.

'If you don't call us back, you'll be arrested.'

Criminals can make a caller ID phone number look like it's coming from anywhere — including the IRS, the local police, or some other intimidating source. But the IRS doesn't leave prerecorded voicemails, especially ones that claim to be urgent or are threatening. Also, the IRS can't revoke your driver's license, business license, or immigration status.

For more tax and IRS scam information, visit https://www.nerdwallet.com/article/taxes/avoid-irs-scams

Source:

City of Winter Springs, February 2024