Mobile Banking App is HERE!

UNION BANK

April 2023

How to Stop Those Annoying Spam Calls You Get Every Day

You shouldn't be afraid to pick up your phone.

You probably receive a handful of calls every day. Not from friends or family, but from scammers and telemarketers, notifying you that you've "won tickets to Hawaii" or pretending to be the IRS and threatening you so you'll pay up.

In January 2023 alone, Americans received 5.51 billion robocalls, which is nearly 20 spam calls for every single person in the US, according to Robokiller, a company that specializes in blocking spam calls and robocalls.

And these calls come in all shapes and sizes. You're likely familiar with the good ol' "scam likely" calls, but there are also more sophisticated attacks that involve spoofing local numbers and those of popular companies, to convince you to give up your personal information and cash. More recently, these attacks have moved over to SMS, where there are phishing text messages that come from your own phone number.

No matter what the calls say, one thing is certain -- they need to stop.

Over the last couple of years, the Federal Communications Commission aimed to wrangle the robocall problem by requiring major wireless carriers to start using Stir/Shaken technology. Stir/Shaken verifies all incoming and outgoing calls for wireless carriers that are routed through their networks. By verifying each call, carriers can reduce the number of fake or spoofed calls. But it only stops robocalls on one avenue -- it's not the be-all and end-all. You may still get spam calls for free trips or fake notices that your student loan payment is overdue.

You can read more about Stir/Shaken here. As the FCC continues its crusade, keep reading this story for things you can do to help curb the number of times your phone rings throughout the day with calls from potential fraudsters.

How to keep annoying robocalls at a minimum

According to the FCC, there are some easy steps you can take to help reduce robocalls:

- Don't answer calls from blocked or unknown numbers.
- Don't answer calls from numbers you don't recognize.
- Don't assume an incoming call is really from a local number just because it looks like it is.

Continued on Page 2

Member FDIC

EQUAL HOUSING LENDER

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
Kroger Plaza 19 Acme Street Marietta, OH 45750
740-374-0010
This is not a full service location. Deposits/withdrawals cannot be processed at this location.

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

- Don't respond to any questions that can be answered with a "Yes."
- If someone calls you and claims to be with XYZ company, hang up and call the company yourself. Use the company's website to find an official number.
- If you do answer a call and hear a recording such as, "Hello, can you hear me?" just hang up.
- The same goes for a call where you're asked to press a number before being connected to a representative.

When you answer a call and interact with the voice prompt or by pressing a number, it lets spammers know your number is real. They can then sell your number to another company or begin targeting your number more frequently.

When it first launched, Google's Call Screen feature arguably went against the FCC's advice by answering and interacting with the robocall on your behalf. However, Google added new features to Call Screen for its Pixel phone lineup. The feature can now detect robocalls and spam calls and block them before they reach you. Google Assistant will interact with the caller, and if it determines that the call is legitimate, it will route the call to your phone.

Apple's iPhone has an option to Silence Unknown Callers, which adds the option to route calls from numbers not found in your Contacts, Mail or Messages straight to voicemail. Any legitimate callers can leave a message. But that's the rub: We often receive important calls from numbers we don't store on our phones, like a doctor's office or a repairman, so you could miss important calls this way. But if all else fails and you're desperate to stop robocalls, this is a valid option.

If you find yourself receiving a lot of spam text messages, you can forward the message to the number 7726 (which spells "spam"). It won't stop the number from texting you right away, but it will allow your carrier to look into where it came from and put an end to it.

Check with your wireless carrier

All four major wireless carriers offer some sort of call-blocking feature. All have a free option and a premium tier.

AT&T ActiveArmor is available for iOS and Android. The free version blocks spam and fraud calls and provides nuisance warning labels and a personal block list, and you can block all unknown callers. AT&T's paid ActiveArmor Advanced offers additional benefits of caller ID for unknown numbers, reverse number lookup, identity monitoring and public Wi-Fi protection.

Verizon's Call Filter app is automatically enabled for Android users on a postpaid plan. The service offers spam detection, a spam filter, a call log for blocked or spam calls, the ability to allow calls from specific numbers (iOS only) and the option to report numbers for free. For a fee, you can get caller ID, spam lookup, a personal block list and a spam risk meter. Call Filter is built into most Android devices out of the box but is also available in the App Store for iOS users.

T-Mobile's Scam Shield is free to all customers and includes multiple features designed to protect you from robocalls and sharing your personal information. Dial #662# from your phone to turn on Scam Block, or download the free Scam Shield app in your phone's respective app store. With Scam Shield enabled, you'll get full caller ID, scam reporting, scam blocking before your phone ever rings and the option to mark numbers as favorites so they still ring your phone.

Use a third-party app to limit the number of robocalls you get

If your provider doesn't offer an app or service to cut back on robocalls, or does but it's too expensive, there are plenty of third-party apps available. You want to find an app that works on your device, offers automatic call blocking and spam alerts for suspicious calls and makes it easy to report a number if a call slips through.

Some options are:

Hiya
Nomorobo
YouMail
RoboKiller
Firewall app

Another option is to get a free Google Voice phone number that you can use to sign up for things instead of giving out your real number -- and once the robocalls start coming in on that Google Voice number, use the block feature. Just know that blocking calls may end up being a lot of work, as robocallers are constantly spoofing different phone numbers.

None of the above solutions is perfect, but they supplement your carrier's integration of technology now required to check for caller ID spoofing. So right now you have to do some extra work to keep the number of robocalls you receive to a minimum. Between being cautious about calls from unknown numbers and using a service (paid or free), you can reduce the amount of unwanted calls and spam you have to deal with.

In sum, carriers have started using Stir/Shaken technology to verify callers, which so far hasn't significantly cut down on the number of robocalls we all receive. So for those with an iPhone, learn where the setting is to block unknown callers, but remember using it could mean you miss calls from doctors' offices and the like. And for those with a Pixel phone, Google's Call Screen feature will surely help, and may even entertain you.

***Source:** cnet.com, Jason Cipriani, Nelson Aguilar, Feb. 8, 2023*

Tax season update: beware of email, text scams

The Internal Revenue Service (IRS) is urging taxpayers to be mindful of scammers using emails and text messages to trick people into providing their personal and tax information. In a press release issued this week, the IRS warned against clicking on or opening emails or text messages claiming to be from the agency, as the IRS never "initiate contact with taxpayers by email, text or social media regarding a bill or tax refund." We're sharing the full press release below for your convenience:

WASHINGTON – With the filing deadline quickly approaching, the Internal Revenue Service today urged everyone to remain vigilant against email and text scams aimed at tricking taxpayers about refunds or tax issues.

In day two of the annual Dirty Dozen tax scams campaign, the IRS again includes a warning about phishing and smishing schemes where cybercriminals try to steal a taxpayer's information through scam emails or text messages.

"Email and text scams are relentless, and scammers frequently use tax season as a way of tricking people," said IRS Commissioner Danny Werfel. "With people anxious to receive the latest information about a refund or other tax issue, scammers will regularly pose as the IRS, a state tax agency or others in the tax industry in emails and texts. People should be incredibly wary about unexpected messages like this that can be a trap, especially during filing season."

As a member of the Security Summit, the IRS, with state tax agencies and the nation's tax industry, have taken numerous steps over the last eight years to warn people to watch out for common scams and schemes each tax season that can contribute to identity theft. Along with the Security Summit initiative, the Dirty Dozen aims to protect taxpayers, businesses and the tax system from identity thieves and various hoaxes designed to steal money and information.

The Dirty Dozen is an annual IRS list of 12 scams and schemes that put taxpayers and the tax professional community at risk of losing money, personal data and more. Some items on the list are new, and some make a return visit. While the list is not a legal document or a formal listing of agency enforcement priorities, it is intended to alert taxpayers, businesses and tax preparers about scams at large.

Phish or smish: Avoid getting hooked by either

Taxpayers and tax professionals should be alert to fake communications posing as legitimate organizations in the tax and financial community, including the IRS and states. These messages arrive in the form of an unsolicited text or email to lure unsuspecting victims to provide valuable personal and financial information that can lead to identity theft. There are two main types:

- **Phishing** is an email sent by fraudsters claiming to come from the IRS or another legitimate organization, including state tax organizations or a financial firm. The email lures the victims into the scam by a variety of ruses such as enticing victims with a phony tax refund or frightening them with false legal/criminal charges for tax fraud.

- **Smishing** is a text or smartphone SMS message that uses the same technique as phishing. Scammers often use alarming language like, "Your account has now been put on hold," or "Unusual Activity Report" with a bogus "Solutions" link to restore the recipient's account. Unexpected tax refunds are another potential target for scam artists.

The IRS initiates most contacts through regular mail and will never initiate contact with taxpayers by email, text or social media regarding a bill or tax refund.

Never click on any unsolicited communication claiming to be the IRS as it may surreptitiously load malware. It may also be a way for malicious hackers to load ransomware that keeps the legitimate user from accessing their system and files.

Individuals should never respond to tax-related phishing or smishing or click on the URL link. Instead, the scams should be reported by sending the email or a copy of the text/SMS as an attachment to phishing@irs.gov. The report should include the caller ID (email or phone number), date, time and time zone, and the number that received the message.

Taxpayers can also report scams to the Treasury Inspector General for Tax Administration or the Internet Crime Complaint Center. The Report Phishing and Online Scams page at IRS.gov provides complete details. The Federal Communications Commission's Smartphone Security Checker is a useful tool against mobile security threats.

The IRS also warns taxpayers to be wary of messages that appear to be from friends or family but that are possibly stolen or compromised email or text accounts from someone they know. This remains a popular way to target individuals and tax preparers for a variety of scams. Individuals should verify the identity of the sender by using another communication method; for instance, calling a number they independently know to be accurate, not the number provided in the email or text."

Read the IRS press release to learn more.

Source: ***City of Philadelphia, Fatoumata Fofana-Bility , March 23, 2023***