

Docs and FAQs

- [So Your Calls are Being Marked as SPAM \(But What If They're Not?\)](#)
- [What is a remote desktop?](#)
- [What is screen sharing?](#)
- [Shared Parking Vs. Park Orbit](#)
- [Which Client? PWA vs Desktop vs Native App](#)
- [Uninstalling the Desktop App](#)

So Your Calls are Being Marked as SPAM (But What If They're Not?)

Oh no! If your customers have stopped answering, it might be because they're seeing calls from your phone numbers displayed as SPAM LIKELY or SPAM RISK via caller ID. Each phone carrier keeps a list of numbers they determine to be spam risks based on the history of the number, crowdsourced feedback and complaint data, and reputation analytics. Some of the most common reasons for getting a spam flag include:



1. The volume of outbound calls per day, per number, is high.
2. Someone flagged a call from your number in their carrier's network database (perhaps before you even bought that new number).
3. The Outbound Caller ID number is not set properly in the invite and if invalid or incomplete, may be marked as spam automatically.

How Does This Happen-And Why Me?!

In response to the growing number of scam calls to mobile phones, many carriers and third parties have created tools to identify and block scam calls. Unfortunately, these tools aren't perfect and they cast a wide net. Businesses may have their numbers incorrectly marked by scam ID technology, particularly when calling cell numbers. There are several technical triggers:

- Carrier spam features/apps that are automatically enabled on mobile devices. When someone calls one of these devices, the carrier checks the number against its database of reported scam numbers. If the source matches a reported scam number, the person being called sees a message that says “Scam Likely” alongside standard caller ID. The user can then decide whether or not to answer the call.
- In addition to “Scam ID,” carriers also allow customers to opt in to a “Scam Block” feature that prevents all Scam Likely calls from ever reaching the user’s phone in the first place. All of the carriers have now introduced their own paid and free versions of this service. Third-party apps also allow smartphone users to detect, report, and block scam calls.
- The Scam Likely Caller ID features will sometimes mark legitimate calls incorrectly, such that some people may report your number without even answering the phone. If this happens enough, your number will be marked Scam Likely.
- Carriers are also deploying algorithms in their networks to detect when a large number of phone calls originate from a common Caller ID number. They designate these calls as SPAM and display a “SPAM” message on the display of the receiving phone.

What to do? It’s critical that you’re able to call your customers and have them answer. Fortunately, there are ways to rectify the situation.

What’s the Fastest Way to Resolve It?

Unfortunately, there is no central database or service so far that manages this number flag, so it can sometimes take a little work to get it corrected. You can also take steps to avoid being flagged from the get-go.

Be Proactive

Encourage your customers to add your main number(s) to their contact lists, which supersede most carrier spam traps and allow calls to be delivered.

Next, register your numbers at the Free Caller Registry via <https://www.freecallerregistry.com/fcr/>. This helps register and whitelist your numbers with several top carriers and reduces the chances of them being flagged. The numbers and information provided will automatically be shared with all three of the Carrier Spam Monitoring Partners, namely HIYA, TNSI, and First Orion.

Getting your numbers registered has shown to be highly effective in protecting them from being flagged for many of the reasons listed above.

Get Your Number Removed from SPAM/SCAM Designations

Contact Carriers

You can use the links or email addresses below to register legitimate numbers and also address any incorrect labeling or call blocking with other carriers:

- **AT&T (HIYA)** https://hiyahelp.zendesk.com/hc/en-us/requests/new?ticket_form_id=824667
- **T-Mobile, Sprint (1st Orion)** <https://calltransparency.com>
- **Verizon, U.S. Cellular (TNS)** <https://reportarobocall.com>
- **Comcast, Charter, Cox, Altice and other fixed-line (VoIP) providers**
Email Nomorobo for call blocking services: reports@nomorobo.com

Popular Spam Blocking Apps

In addition, here are some of the most popular spam blocking apps and contact info if you wish to reach out about being unflagged on their apps.

- **Robokiller** – Most popular call blocking app, millions of people have this application. Once you are blocked by them, every single user with the app will automatically have your number blocked. Email support@robokiller.com.
- **Nomorobo** – No Scoring/Rating System. Very Popular Call Blocking App. Winner of FTC Robocall Challenge. Email reports@nomorobo.com.
- **Icehook** – Will be marked as spam if it falls into “highly likely” / 81-100 risk level range. Contact them at <https://www.icehook.com/contact>
- **TrueSpam** – Uses a 0 – 100 Scale; flags occur with a score of 60+. Contact Info: https://www.truecnam.com/contact_us
- **Telo** – Nuisance score flagged at 65+, at which point they’ll notify you before your number is labeled a nuisance-level call at 70+. Contact <https://www.telo.com>

Third-Party Services

Last but not least, there are third-party services that can help get your numbers clean and keep them clean. For example, look into Caller ID Reputation Services like <https://calleridreputation.com/>, or Numeracle’s [Entity Identity Management](#) platform, which prevents as well as remediates incorrect call blocking and labeling events

by Katie Reddick | May 24, 2022 | <https://tinyurl.com/s27nj92p>

What is a remote desktop?

A remote desktop is a program or operating system feature that enables your device to be remotely accessed or controlled by a user in a separate location from a separate PC or mobile device. Remote desktops can be used in sales, support and customer service functions to offer advice and guidance to clients. Remote desktop access functionalities include:

- Troubleshooting / Fixing Hardware Issues.
- Performing hands-on demonstrations.
- Installing and updating software.
- Accessing workplace computers whilst working remotely.

Why should I invest in remote desktop software?

Use the WebMeeting Remote Control client to connect to and control a computer remotely from anywhere around the world. The Remote Control client enables secure and reliable remote Windows desktop connections for both IT professionals and everyday users, to provide assistance, support, or demonstrate your products and services on remote PCs. Simply have the meeting participant install the WebMeeting Remote Control client on their machine and quickly start your remote control session within 5'.

Screen Sharing in a Web Meeting - Screenshot

Are remote desktops secure?

It's important to choose a remote desktop application from a trusted provider in order to guarantee that your data and other sensitive material remains protected. When choosing your remote application, make sure that remote sessions are encrypted and only accessible by authorised users. Never grant remote access permissions to a user who contacts you first. Where possible, only allow a trusted IT partner to conduct viewing sessions.

Would I need to install software on both devices?

Until fairly recently, to setup remote access you typically need to install and configure various software components and libraries on both machines; the controller and the one controlled BEFORE access could even be requested. This made troubleshooting on the behalf of clients cumbersome and time-consuming. However, with the introduction of Google's WebRTC protocol, things became a lot simpler! Using only a web browser and a secure video conferencing solution you can now initiate a remote desktop session in just a few clicks. All that's required is for the controlled PC to download a simple plugin before access can be enabled. Say goodbye to remote desktop clients and complex installs!

What remote control functionality does 3CX offer?

The video conference solution for business by 3CX has an inbuilt remote control feature that can be used to connect to and control a computer remotely from anywhere in the world. The Remote Control client offers secure and reliable remote Windows desktop connections for both IT professionals and everyday users. Use it to provide assistance, support, or demonstrate your products and services on remote PCs. Just fire-up 3CX WebMeeting and send a request to remotely control any of the invited participant's PCs. There's no specialist software required, just a quick to install plugin for the PC that's going to be controlled. Then, use WebMeeting's file sharing feature to transfer, backup and restore mission-critical files.

Key features

- Initiate remote control through WebMeeting.
- Simple and quick installation.
- Compatible with Windows security framework and UAC (User Account Control).
- Record remote control sessions and share with participants.
- File transfer via built-in WebMeeting file sharing.
- Shared local-remote clipboard.
- GPU-acceleration for better performance.
- Low system resource usage.

What is screen sharing?

Screen Sharing or desktop sharing technology enables you to share your entire screen or a specific window with other computers. Using specialist technology or plugins, presenters can give remote users permission to view on-screen activity from their own device. Screen sharing is sometimes confused with 'Team Viewing' or [remote desktop capabilities](#). Whilst all three techniques allow a remote device to view a computer screen, screen sharing technology does NOT grant permission to control or make changes to the viewed computer. For this reason, screen sharing is primarily used as a collaboration and presentation tool. In this capacity, it can dramatically improve your sales, support and customer service!

Screen Sharing
Image not foundtype unknown

What are the applications of screen sharing?

Perfect pitches and meetings

Executing the perfect sales pitch over the phone can be tough, but it doesn't need to be. Desktop sharing makes it possible to show remote attendees everything your business offers without even leaving the office. Take prospects virtually by the hand and guide them through your product or service offerings. Whether you need to carry out meetings or present pitch decks and sales presentations, you will save time and expense by conducting them remotely using screen sharing in conjunction with your video conferencing solution.

Train customers and staff effectively

Easily roll out new products and services across your business sharing your desktop with multiple meeting participants. The physical limits of the office are no longer a barrier as you use screen sharing to collaborate with team members in real-time, regardless of where they are located in the world! By sharing the same screen content, such as an image, a graph, or a chart, your participants can see exactly what you are referring to avoiding any confusion or misunderstanding.

Boost your customer service

Screen share can also be used in a customer service or support capacity. Troubleshoot customer and colleagues queries, regardless of the distance between you! Your employees can be in any location and can still collaborate and learn from fellow team members. Additionally, customers who need assistance with new software, working through technical problems, or changing settings can use a screen sharing feature to have a 1-1 conversation with a technical advisor who can walk them through step by step.

What are the benefits of screen sharing?

Using a screen sharing feature saves time and money. Rather than having to travel to your client's site each time you want to discuss a new sales opportunity or offer training, you can conduct the session remotely without needing to worry that key information will get lost in translation. By incorporating sharing alongside your video conferencing solution, you'll reduce local travel and the need for overseas business trips- just imagine the financial and environmental benefits! Invite your customers to a web meeting, begin sharing your screen and interact with them as if you were face to face.

What does 3CX offer?

3CX's integrated secure video conferencing software transforms two-dimensional audio communication into an interactive, audiovisual experience that makes meetings more productive. Simply launch or schedule your WebMeeting session, invite the desired participants and click the screen share icon to get started! You can even screen-share with video and audio playback to add some flair to your presentations! There's no need to purchase any additional software or install a plugin, all that's required is an active internet connection and a google chrome or safari web browser.

Key features:

- Share your desktop and other applications
- Easy to use
- Share documents and files
- Text chat and file transfer
- Whiteboard feature
- Screenshare with Audio

Shared Parking Vs. Park Orbit

A question 3CX support often gets asked is, “What is the difference between shared parking and the park orbit?”. Overall, there are no differences in regards to what they both offer. Both are “slots” in which calls can be placed and retrieved. However, behind the scenes there are some vast distinctions between the two. Let’s untangle the cord.

Parking Orbits

Imagine parking orbits as “rooms” within 3CX. Calls can be placed into these “rooms” by transferring them from your IP phone or 3CX client. There are 10 rooms available and shared, unrestricted, between all users. A max. total of 64 calls can be placed into those rooms. Wait, 64 calls in 10 rooms? How does this work?

Get in

To park a call into a room press the transfer button on your SIP device followed by entering the number *0[0-9] (eg *00). The active call on your extension will be placed into room 0. The transferred party will be placed on hold.

It is possible to keep transferring more calls into *00, from your extensions or others, or to *01 even if there are calls in the room already. Don’t worry, calls held in a room cannot talk to each other, otherwise you would be in a conference call.

Get Out

To unpark a call which is parked in a room, create a new call from your SIP device to *1[0-9] (eg *10).

It is important to know that each and every extension in 3CX can unpark calls which have been parked by someone else. If the CEO parks an important business partner into a room, this call can be resumed by every other user of the system.

In the case that in a single room multiple calls have been parked, the call that was parked first will be retrieved first while using the matching dial code of the room (*10 for room 0). In case you need to selectively unpark a person from a room with multiple calls in it, you must use the 3CX client for Windows or Mac or the Web Client to do so.

Use Case I

I get a call from person A who needs to urgently talk to a colleague of mine. After an attempted transfer, I failed to get the requested colleague on the line. I decide to physically go and find the colleague in question. While I get up to go find the colleague, I place the caller into *00 and hang up my phone. Once I find the person I am looking for, who often happens not to be in their office, any SIP phone close to him/us will do the job. I dial *10 and hand over the call to my colleague. The result? A happy customer...

Use Case II

I have a SIP forked ID (meaning I have more than one SIP device on my extension) with a DECT phone and my 3CX client. I take a call on my 3CX client but I need leave my desk whilst on the call. So how do I transfer the call from me to myself? I transfer the call to *05 and then dial *15 on my DECT phone and I am good to go.

Shared Parking

Compared to the open parking space above, in shared parking the call flow is much more controlled. Firstly, there are 250 rooms and they are called SP[0-250].

These rooms can be provisioned onto a SIP device (3CX client and IP phone) which will give visual feedback about the state of the room (free or busy) on the respective BLF key. By simply pressing on the matching BLF key a call can be placed into a room and all extensions monitoring the same room on their SIP device will see that there is a call up for grabs.

There is also a limit of 1 person per room. Shared parking is a sort of replication of “shared line appearance” which you may be familiar with. Additionally, if you use the park function from the 3CX client or Web Client those calls will be placed into shared parking slots in an ascending free order.

Shared Parking Orbit of calls

Use Case

Assume that the reception has been tasked to distribute calls to the internal staff. For each member of staff a dedicated shared parking slot was allocated and provisioned onto their SIP device. On incoming calls the reception can monitor whether or not the requested person is available via the 3CX Switchboard. If not, instead of “terminating” the call, the call can be placed in the SP slot of the person. Once the person finishes their current call, the BLF on the person's SIP device indicates the next call to process which can be taken via a simple press of the BLF button.

Which Client? PWA vs Desktop vs Native App

Web client with BLE unknown

Many users followed our advice to deploy our PWA web app mode instead of our Desktop App during the attack. Following this, we learned more about deploying in this mode. I wanted to share some of the things we've seen and give some background and suggestions on which is the best to use according to the situation.

The PWA (Progressive Web App) app

What is a PWA app?

PWA stands for [Progressive Web Apps \(PWAs\)](#). These are applications built using web technologies that can be installed and run on all devices from one codebase - in this case, our Web Client - which is also the basis for our Desktop App. A PWA provides native-like experiences and adapts to the capabilities supported by each device. Some characteristics:

- Works on Chrome and Microsoft Edge Chromium.
- Runs securely within the browser in its security framework and libraries.
- Zero admin - automatically updates.
- No local installation needed - no install or uninstall.
- Runs in the background and supports Push Notifications.

What does the 3CX PWA app do

- Fully functional 3CX client that feels/looks like a native app.
- Starts automatically upon starting the browser.
- Notifies user of incoming calls via a PUSH notification message box.
 - No need to be logged in to 3CX or even have the tab open.
 - In case of Edge, browser will be started if not active.

- In the case of Chrome browser must be running.
- Launch calls in CRM or websites via Click2Call extension.
- Calls can be auto answered.
- Supports SSO.
- Fully supports Yealink, Jabra and soon Plantronics headsets.
- PWA works great on Microsoft Terminal Server - Read how to [mass deploy](#).
- To be added in update 7a: Dialer will include the BLF panel.
- To be added in update 8: Be launched via the tel: protocol by 3rd party external apps.

PWA - Must haves \ Must dos

- PWA will only work for installations that have a fully qualified domain and a valid SSL certificate.
 - If you host 3CX in the cloud using a 3CX certificate, this is automatic.
 - If you have an on-premise installation, you must have configured Split DNS with a valid 3CX certificate or custom certificate. You are gonna need this anyway, sooner or later!
- You must set Google or Edge to auto start upon login to the OS. Here's [how](#).

What PWA can not do

- Capture focus on incoming calls - Unfortunately, we have not found a way around this.
- Microsoft Tapi Integration for some older CRM/Accounting applications such as Datev.
- Launch External Applications upon receiving a call.

Desktop App

What is the Desktop App (also referred to as the Electron app)? The desktop app is a repackaged web client using the [Electron framework](#). It allows control of the browser version of the browser as well as access to operating system functions.

It was this app that got compromised in the 3CX supply chain attack. This had nothing to do with the Electron framework or indeed any of the components we shipped in the Desktop app. The Desktop App was compromised because our network had been attacked by a hacker group. Our investigator Mandiant assesses with high confidence that UNC4736 has a North Korean nexus.

Read more about this [here](#).

The compromised Desktop App has since been completely checked and cleaned and can be considered secure. We have put controls and procedures as well as tools in place to ensure supply chain attacks will not hit us again.

What the Desktop App can do in addition to the PWA

- Capture focus on incoming calls.
- Launch External Applications upon receiving a call.
- Dial or transfer using hotkeys.
- Allow for the dialer dialog to be moved around the screen separately from the main screen.

What the Desktop App can not do

- TAPI - ability to be launched by TAPI capable apps.
- If you close the app, then you will not be notified of incoming calls.

What the Desktop App requires

- Network wide antivirus and controls in case of emergency

Native App

3CX has native apps for all major operating systems - iOS, Android and Windows. These apps use SIP rather than WebRTC for calls. They operate entirely separate from the PBX using SIP authentication IDs rather than web authentication. This means that the maximum a hacker can do if it obtains access to these credentials is make and receive calls.

Whilst the iOS and Android apps are distributed via their app stores, the Windows app is distributed via the PBX. Currently, the native Windows app is also referred to as our [Legacy app](#). This app works well and is secure, but has not been updated in a while. During the supply chain attack, this was a godsend. However, its architecture is out of date and needs to be redone.

We're now considering developing a new native Windows app that will look and behave like the iOS and Android apps. It would be distributed via the Microsoft store. This makes it inherently secure not only because the store checks the security of the apps before uploading, but also because in case of a security event, it allows for a much faster and automatic response.

What the Native App can do in addition to Desktop or PWA app

- Capture focus on incoming calls.
- Launch External Applications upon receiving a call.
- TAPI - ability to be launched or be launched from TAPI capable apps.

What the Native App requires

- Local admin rights to install the app.
- Provisioning via PNP on local LAN OR download of config file (U8).

Uninstalling the Desktop App

The Desktop App can be uninstalled as explained below. On some Windows machines where antivirus software already deleted some of the files the uninstaller may fail.

On Windows:

1. Start
2. Type "Control Panel", Enter
3. Select "Programs and Features"
4. Find 3CX Desktop App, select and press "Uninstall".

On Mac:

1. Go to "Applications"
2. Tap on "3CX Desktop APP"
3. Right click then "Move to Bin"
4. Ensure that it isn't also present on Desktop otherwise delete it from there as well.
5. Empty the Bin

Mass / Network Uninstall of Electron App

Partners on our forums have kindly contributed Powershell scripts that allow companies to mass uninstall the electron app from their Network. We have merged them into one that will attempt to uninstall and forcibly delete any remaining files and entries associated with the Desktop App. We hereby thank the original authors of the scripts that were merged. This powershell script hasn't been thoroughly tested yet from our end, we recommend testing it on one machine first before executing it on your customers infrastructure. This must be run on client machines not the server.

Important: There are many scripts being suggested on the internet. Please be careful with any script or executable found on the internet, do not blindly trust them as they may be harmful.

```
# Kill 3CX processes first
```

```
Get-process | Where-Object {$_.name -Like "*3CX*"} | stop-process
```

```
# Attempt #1 - via EXE uninstall method
```

```
$3cxapps = Get-WMIObject -Class Win32_product | where {$_.name -like "3CX Desktop APP"}
```

```
foreach ($app in $3cxapps) {
```

```
try {
```

```
$app.Uninstall()
Remove-Item C:\Users\$env:UserName\AppData\Roaming\3CXDesktopApp -Recurse
Remove-Item C:\Users\$env:UserName\AppData\Local\Programs\3CXDesktopApp -Recurse
Remove-Item C:\Users\$env:UserName\Desktop\3CX Desktop App.Ink -Recurse
Write-Host "Uninstalled $($app.Name)"
}
catch {
Write-Host "Error uninstalling $($app.Name): $($_.Exception.Message)"
}
}

# Attempt #2 - via MSIEXEC ~ Requires Set-ExecutionPolicy to be changed
$appInstalled = Get-WmiObject -Class Win32_Product | Where-Object {$_.Name -eq "3CX Desktop App" }
if ($appInstalled) {
try {
$uninstallString = $appInstalled.UninstallString
Start-Process msixexec.exe -ArgumentList "/x `"$uninstallString`" /qn" -Wait -NoNewWindow
Remove-Item C:\Users\$env:UserName\AppData\Roaming\3CXDesktopApp -Recurse
Remove-Item C:\Users\$env:UserName\AppData\Local\Programs\3CXDesktopApp -Recurse
Remove-Item C:\Users\$env:UserName\Desktop\3CX Desktop App.Ink -Recurse
Write-Host "Uninstalled $($appName)"
}
catch {
Write-Host "Error uninstalling $($appName): $($_.Exception.Message)"
}
}
else {
Write-Host "$appName is not installed"
}
}
```