Auto Attendant

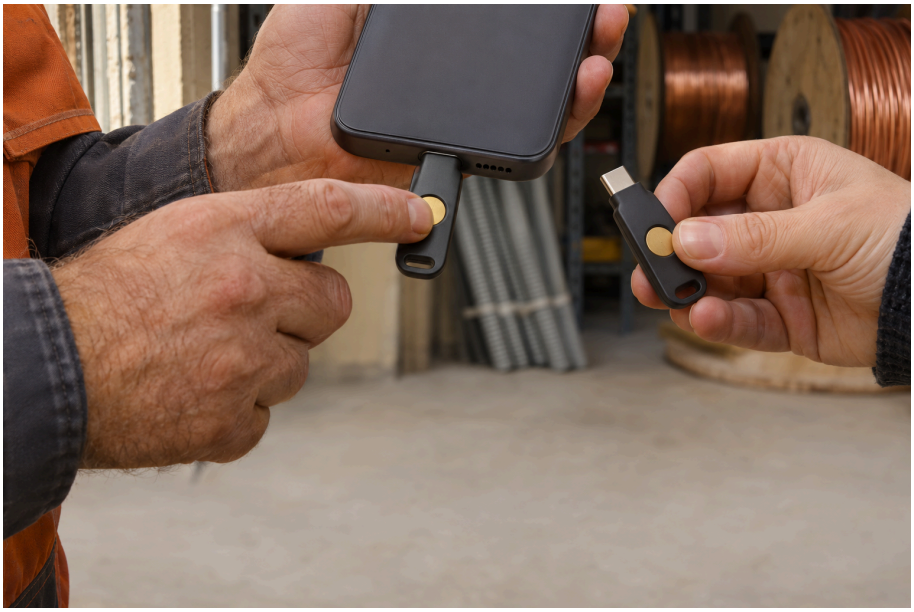
AUTO ATTENDANT / RESEARCH & PRACTICAL GUIDANCE

Business Phone Number for 2FA: Which Sign-Ins Should Use It?

> Get a business phone number with a simple auto attendant menu from Auto Attendant. A caller picks who they need and the call rings that person's own mobile, so nobody on your team has to publish a personal number.

Published by Auto Attendant · 2026-11-13 · business phone number for 2fa · voip two-factor authentication · sms verification codes · line type · account recovery phone · authenticator app vs sms · auto attendant · small business security

Original article: https://autoattendant.io/articles/business-phone-number-2fa-sign-ins



In this article

1. Executive Summary
2. Introduction and Background
3. Line Types and Why Platforms Treat Them Differently
4. How a Code Actually Reaches a Person
5. The Per-Account Worksheet
6. What to Put Instead of the Business Number
7. Recovery, Ported Numbers and Departing Staff
8. Data Analysis and Evidence
9. Case Studies and Real-World Examples
10. Implications and Future Directions
11. Frequently Asked Questions (FAQs)
12. Conclusion

Executive Summary

Whether a code sent to a business number ever reaches a person depends on three things: how the platform classifies the line, whether the code can arrive by voice as well as text, and who or what answers when it arrives. This report turns those questions into an account-by-account worksheet for small businesses in the United States and Canada. It is platform-policy based, and it names the jurisdiction wherever a rule is national.

The first finding is that no universal rule exists. Microsoft's help page for personal accounts says **VoIP numbers cannot be added** for sign-in or verification codes (support.microsoft.com). Indeed says it **no longer allows non-fixed VoIP numbers** for account verification, OpenAI's help article says landlines, VoIP and Google Voice numbers are **not supported** (help.openai.com), and Upwork says it cannot verify VoIP numbers (support.upwork.com). Google's own "cannot be used for verification" page, by contrast, attributes the error to limits on how often a number can be used and tells the user to try a different number (support.google.com). The banks and payroll providers reviewed here (RBC, Wells Fargo, Gusto and Paychex) list delivery methods without stating a line-type policy.

The second finding concerns delivery. Google's Business Profile help states that **phone menu (IVR) systems will not get the code** (support.google.com), and Twilio's help center says a voice-delivered code needs a live answer and cannot sit behind an extension or go straight to voicemail (help.twilio.com). A number whose job is to present a menu is therefore a poor default recipient for automated verification calls.

The third finding is that the standards direction favors fewer phone dependencies. NIST SP 800-63B-4 (final, 31 July 2025) calls PSTN out-of-band codes "one restricted authenticator" and requires verifiers to make alternatives available (pages.nist.gov). It is a U.S. federal digital-identity standard, not a law binding private platforms. Google's 2019 study found an SMS code blocked 100% of automated bots, 96% of bulk phishing and 76% of targeted attacks, against 100%, 99% and 90% for on-device prompts (security.googleblog.com).

The recommendation is a three-way split: an authenticator app, passkey or security key wherever offered; a carrier-issued mobile held by a named owner and a deputy where a phone is required; and the shared business number only where the platform's page accepts it and the delivery test passes. Table 2 records each choice with its backup.

Introduction and Background

Owners setting up or porting a business number usually enter it as the "verification phone" on a dozen accounts in the first week: email, domain registrar, bank, payroll, payment processor, advertising, marketplaces, hiring platforms and accounting software. The decision looks trivial, but the number serves two jobs at once: a public contact point that callers reach through a menu, and a recovery channel that must reach one accountable person at an unpredictable moment.

This report does not repeat the security argument for removing a business number from text-message sign-in, covered on the publisher's port-out and SIM-swap research page, nor one platform's code flow, covered in the WhatsApp article, nor the general calls and texts checklist. Its job is narrower: a per-account decision built on line type and on how a code physically reaches a person when the number sits behind a menu.

Scope, jurisdiction and evidence rules

Every platform statement here comes from the platform's own help page or documentation, opened on 13 November 2026. Where a page does not mention VoIP or line types, the report says so rather than inferring a policy, and bank or payroll policies are not generalized from one institution to another. NIST, CISA, the FTC and the FCC are U.S. bodies; the Canadian Centre for Cyber Security supplies the Canadian guidance. No CRTC (Canadian Radio-television and Telecommunications Commission) source could be retrieved, so no Canadian porting or SIM-change rule is asserted. NIST's guideline governs U.S. federal digital-identity systems; this report uses it as a signal about direction, never as a legal duty on a private platform.

The three questions

Before a number goes into any account, three questions decide whether it is a good fit:

- **Does the platform accept this line type?** Look for first-party help text, not a blog's summary.
- **Can the code arrive by voice as well as text?** A landline cannot natively receive SMS, and some platforms offer only SMS.
- **Who physically receives it?** A named person's phone, a shared voicemail box and a menu are three different answers.

Line Types and Why Platforms Treat Them Differently

Lookup vendors sell a "line type" check that platforms can run on a number at sign-up, and the categories those lookups return explain most of the rejections owners meet.

The categories in plain language

Twilio's Lookup documentation, one commercial vendor's taxonomy, defines the types most relevant here. A **landline** generally cannot receive SMS (www.twilio.com). A **fixed VoIP** (voice over internet protocol) number is a virtual number associated with a physical device (www.twilio.com). A **non-fixed VoIP** number is a virtual number obtained online without requiring a physical device (www.twilio.com). A **toll-free** number is one where calls are free for the calling party (www.twilio.com). Mobile numbers, the fifth common type, are the ones that generally can receive SMS.

Bandwidth, a carrier-grade number provider, frames the same split by registration: a non-fixed VoIP number has no registered address (www.bandwidth.com). It adds that some landlines are text-enabled through hosted messaging (www.bandwidth.com), so "landline" does not always mean "cannot text". The FCC describes interconnected VoIP services as those that let users generally make and receive calls on the regular telephone network (www.fcc.gov), so a VoIP line can place ordinary calls and still be classified differently from a mobile.

Table 1 below summarizes the categories. The treatment column is deliberately labeled "varies; check help page", because platforms set their own policies.

Line type	What it is (vendor definition)	Can usually receive SMS?	Can usually receive a voice call?	Typical platform treatment
Mobile	A carrier-issued line tied to a SIM or eSIM	Yes, generally	Yes	Most widely accepted; some platforms accept only this type
Landline	A wired line	Generally no; some hosted-messaging exceptions (www.bandwidth.com)	Yes	Varies; check help page. Some offer voice delivery to landlines (go.paychex.com), others do not (kdp.amazon.com)
Fixed VoIP	A virtual number associated with a physical device	Not guaranteed	Yes	Varies; check help page. Indeed accepts fixed VoIP
Non-fixed VoIP	A virtual number obtained online without a physical device	Varies	Yes	Varies; check help page. Several platforms say it is not accepted (support.upwork.com)
Toll-free	Calls are free to the caller	No source reviewed; ask the provider	Yes	WhatsApp lists toll-free numbers as unsupported for registration (faq.whatsapp.com); most other pages are silent

Table 1 is a map of vocabulary, not a verdict. Each "treatment" cell cites the platform that wrote the statement and does not generalize beyond it: a line type is an input to a platform's policy, and the same number can be accepted on one site and rejected on the next.

Why one site rejects what another accepts

Platforms can look a number up. Twilio's documentation says a customer can filter out landline numbers before sending SMS messages (www.twilio.com), and Telnyx describes using lookups to flag number types such as VoIP and non-fixed during signup (developers.telnyx.com). Indeed's published rule acts on the distinction: it accepts mobile, landline or fixed VoIP numbers and no longer allows non-fixed VoIP (www.indeed.com).

Rejection is not always about line type. Google's page for the "This phone number cannot be used for verification" error says Google limits how many times a number can be used for verification and suggests a number from a friend, family member or a different carrier (support.google.com). It says nothing about VoIP. Many third-party summaries claim Google blocks VoIP numbers; Google's own page as opened does not, and this report does not repeat the claim.

What the owner cannot see

The reader usually cannot see how their number is classified, and classification data differs by vendor and country:

- **Bandwidth:** line type reflects carrier records, and porting to a new carrier can change it (www.bandwidth.com).
- **Sinch:** port-corrected data applies to the U.S. and Canada only (developers.sinch.com), and its optional VoIP signal sorts each carrier into one of four likelihood categories (developers.sinch.com).
- **Plivo:** VoIP detection is not supported outside the U.S. (old-support.plivo.com).

Two consequences follow. A reader told "VoIP" should ask the provider whether that means fixed or non-fixed, and Indeed's own advice for a rejected valid number is to contact the carrier to confirm the line type is configured correctly (www.indeed.com). And a number can change category after a port, so a verification that worked before deserves re-testing. This report states no provider's classification; the answer is "ask your provider".

NIST's position is worth separating from platform practice. The change log of SP 800-63B-4 says the revision removes the prohibition on the use of VoIP phone numbers for out-of-band authentication (pages.nist.gov). The standard therefore does not require platforms to reject VoIP numbers; any rejection is a platform's own risk decision.

How a Code Actually Reaches a Person

Accepting a line type is only the first gate. The second is delivery: a six-digit code must land in front of a human who can type it within a short window. For a number that sits behind a phone menu, that is where most failures are likely to occur.

SMS, voice and the menu trap

Most platforms offer text first and voice second. Google says codes can be sent in a text message or a voice call (support.google.com), Twilio calls voice its primary backup to SMS (www.twilio.com), and Square, Intuit and Paychex list voice or automated-call delivery in their own help pages (squareup.com)

(quickbooks.intuit.com) (go.paychex.com). Speed is not guaranteed: Facebook's help notes that text codes can be delayed by the mobile carrier (www.facebook.com).

The menu trap is an automated voice call meeting a number configured to answer with a menu. Three first-party statements support the concern:

- **Google Business Profile:** the help page says that Interactive Voice Response (IVR) systems will not get the code (support.google.com).
- **Twilio help center:** a voice-delivered code requires the user to answer a live phone call, and the number cannot be behind an extension or go straight to voicemail (help.twilio.com).
- **Twilio authentication channels:** the Verify API challenges the answerer with a random keypad digit before reading the token (www.twilio.com), a design intended to confirm that a person rather than a machine is on the line.

Two further statements show the voicemail variant. Google's troubleshooting page says that a voice call carrying a verification code goes to voicemail if the user cannot answer or lacks an adequate connection (support.google.com). WhatsApp's help says that, for the phone call option with voicemail enabled, its automated system will leave the code as a voicemail (faq.whatsapp.com), and that landline extension numbers cannot be used to complete registration (faq.whatsapp.com).

These sources do not describe every platform, but they show menus, extensions and voicemail are recognized failure points for at least three large ones, so testing before enrolment is prudent. A shared voicemail box is the sharper risk: a code left there is readable by everyone with access and by no one in particular.

The six-step code delivery test

This practical procedure, not documented behavior of any platform, answers what a help page cannot: what will happen on this specific number.

1. **Text test.** From a second phone, send a text to the business number and confirm who, if anyone, receives it. A number that cannot receive text cannot use SMS delivery.
2. **Voice test.** Call the number from a second phone and note exactly what answers: a menu, a greeting, a person, or voicemail.
3. **Withheld caller ID test.** Call again from a withheld number. Automated verification calls often arrive without a recognizable caller ID, and some menus or call filters treat such calls differently.
4. **Menu-active test.** During business hours, with the menu live, repeat the call and wait through the greeting without pressing anything. An automated caller cannot choose option 2.
5. **After-hours test.** Repeat after the closed greeting starts. Many menus play a closed message and offer voicemail, which means no human receives the call.
6. **Owner's phone off test.** Switch off the phone that would ring and repeat. If the call falls to a shared voicemail, record who can hear it.

If steps 2 to 6 do not end in a named person's live answer, the number should not receive voice codes for any account. If step 1 fails, mark it "no SMS".

An honest note on routing-first numbers

A number built to route inbound calls to team mobiles through a menu is optimized for callers, not automated systems. The publisher sells one such product, a flat-rate number with a multi-option auto attendant that rings each option's team phones, as described on its own site in November 2026; this is the publisher's self-description, not independent evidence. On that site, after-hours calls are not forwarded to mobiles; callers hear a closed message and can leave voicemail. Whether a platform accepts such a number, and whether a code call survives the menu, must be tested, not assumed. The product page does not state how its numbers are classified, so the answer is to ask the provider. For many accounts, a number of this kind is the wrong verification phone.

The Per-Account Worksheet

Table 2 below is the fillable worksheet. The first four columns are seeded from first-party help pages opened on 13 November 2026. The last column is left blank for the reader: method chosen, named owner, and backup. Cells marked "ask/verify" mean no first-party page stating the policy was opened, so no policy is claimed.

Account category	What the phone is used for	What the platform's own page says (opened 13 Nov 2026)	Documented non-phone alternatives	Suggested default	Your entry: method / named owner / backup
Email (Google Account or Workspace)	Sign-in code, recovery	Needs a mobile device to verify (support.google.com), though the call option accepts a home phone (support.google.com). Advises against a Google Voice number for recovery (support.google.com)	Passkeys (support.google.com) and backup codes (support.google.com)	Passkey or key plus owner and deputy mobiles; business number not recommended	
Email (Microsoft account)	Sign-in code, recovery	VoIP numbers cannot be added for sign-in or codes (support.microsoft.com)	Authenticator app and other non-SMS options; SMS is being phased out for personal accounts (support.microsoft.com)	Authenticator app plus carrier mobile	
Domain registrar	Sign-in code	GoDaddy: a telephone service such as Google Voice cannot be used for SMS (www.godaddy.com); Namecheap accepts any TOTP app (www.namecheap.com); Cloudflare issues one-time backup codes (developers.cloudflare.com)	Authenticator app, passkey or security key	Authenticator app or key held by two people	

Account category	What the phone is used for	What the platform's own page says (opened 13 Nov 2026)	Documented non-phone alternatives	Suggested default	Your entry: method / named owner / backup
Bank or credit union	Sign-in code, transaction approval	RBC (Canada): text to a mobile or a call (www.rbcroyalbank.com), Canadian or U.S. number (www.rbcroyalbank.com); Wells Fargo (U.S.): push, text, email or call (www.wellsfargo.com), text shown for mobile numbers on file (www.wellsfargo.com). Others: ask/verify	Push in the bank's app (Wells Fargo)	Owner's carrier mobile; ask the institution which line types it accepts	
Payroll	Sign-in code, recovery	Gusto: code by text, call or WhatsApp (support.gusto.com); Paychex's October 2026 Oasis guide accepts a landline able to receive calls (go.paychex.com). Others: ask/verify	Authenticator app and passkeys (Gusto)	Authenticator app; named payroll admin plus deputy	
Payment processor	Sign-in code, recovery	Stripe ranks methods most to least secure (support.stripe.com); Square needs a mobile number or an authentication app (squareup.com); PayPal's U.S. page describes an authenticator app (www.paypal.com)	Passkeys, keys, apps (Stripe); authentication app (Square)	Authenticator app or key; backup codes stored offline	
Advertising (Google Ads)	Sign-in code	Lists call, authenticator, prompt, security key and text; Google says Authenticator is more secure than SMS (support.google.com)	Authenticator, security key, prompt	Authenticator or key	
Advertising (Meta)	Sign-in code on new devices	Two-factor is a requirement for business portfolios that are 90 days or older (www.facebook.com); Facebook says the two-factor number cannot also reset the password (www.facebook.com)	Security key, authentication app, 10 recovery codes (www.facebook.com)	Authentication app; second recovery path on a different number or email	
Google Business Profile	Verification call or text	IVR systems will not get the code (support.google.com); Google picks the method and it cannot be changed (support.google.com)	None stated on the page	Verify from a number or device a person answers; run the delivery test first	
Hiring platform	Account verification	Indeed: non-fixed VoIP not allowed (www.indeed.com); Upwork: not able to verify VoIP, use a non-VOIP number (support.upwork.com)	Not stated for the verification step	Owner's carrier mobile	
Accounting software	Sign-in code, recovery	Intuit: text or automated voice codes (quickbooks.intuit.com), and a number change turns two-step verification off (quickbooks.intuit.com); Xero: backup email or security questions (central.xero.com)	Passkeys and apps (Intuit); authenticator app (Xero)	Authenticator app; document the re-enrolment step	

Account category	What the phone is used for	What the platform's own page says (opened 13 Nov 2026)	Documented non-phone alternatives	Suggested default	Your entry: method / named owner / backup
Marketplace or storefront	Sign-in code	Amazon KDP: no voice codes to landlines (kdp.amazon.com); Etsy: app, call or text (help.etsy.com); Shopify: SMS cannot be set up as a new method (help.shopify.com)	Authenticator app (all three)	Authenticator app; backup codes	
AI and developer accounts	Required phone step	OpenAI supports mobile numbers only; landlines, VoIP and Google Voice are not supported (help.openai.com), and an authenticator app does not replace the phone step (help.openai.com)	None for that step	A named person's carrier mobile	
The phone provider itself	Account login, port approvals	No first-party page opened: ask/verify	ask/verify	Owner plus deputy; non-phone recovery email	

Table 2 shows a pattern: platforms that state a line-type rule are in the minority, while nearly every page lists at least one non-phone alternative, so the suggested defaults lean toward alternatives. Rows marked "ask/verify" are open tasks: ask the platform which number types it accepts before enrolling the shared business number.

What to Put Instead of the Business Number

The decision for each account is one of three options: the business number, a carrier-issued mobile held by a named person, or no phone at all. This section walks through each, with the standards signal behind the third.

Option A: the business number

The shared number is a sensible recipient only when all of these hold:

- **Accepted type:** the platform's page accepts the line type.
- **Live human:** the delivery test ends in a person, not a menu or voicemail.
- **No better option:** the platform offers nothing stronger.
- **Accountable owner:** a named person is responsible for what arrives.

A shared voicemail fails the last condition. NIST's authenticator guidance expects users to maintain their own unique authenticators (pages.nist.gov) while acknowledging, with a family phone as the example, that sharing happens in practice (pages.nist.gov). The Canadian Centre for Cyber Security advises minimizing or eliminating shared accounts (www.cyber.gc.ca) and lists changing shared or group authenticators when members leave among the practices it describes (cyber.gc.ca).

Option B: a carrier-issued mobile held by a named person

Where a platform insists on a phone, a mobile held by a named owner solves delivery and accountability together. Google's recovery guidance reads this way: a mobile phone that gets text messages and belongs only to the user (support.google.com). Apple suggests a trusted number not associated with the iPhone as an additional one (support.apple.com). A deputy's mobile as a second number covers one person's absence, and the Canadian Centre advises a backup factor identical in strength to the primary (cyber.gc.ca).

Option C: no phone at all

Authenticator apps, passkeys and security keys remove the number from the equation. The FIDO Alliance describes passkeys as phishing-resistant and designed with no shared secrets (fidoalliance.org), and CISA states that the only widely available phishing-resistant authentication is FIDO/WebAuthn (cisa.gov). Google's passkey help says a passkey bypasses the second authentication step (support.google.com). CISA tells businesses to aim for a phishing-resistant method (www.cisa.gov), the FTC says to require multi-factor authentication for all employees, contractors and others who access the network (www.ftc.gov), and the Canadian Centre strongly recommends FIDO-based solutions for online accounts (cyber.gc.ca). The UK's National Cyber Security Centre adds that any type of two-step verification is better than none (www.ncsc.gov.uk).

Whichever method is chosen, keep a backup. Google's backup codes work once each (support.google.com); Bitwarden advises saving the recovery code immediately after enabling a two-step method (bitwarden.com); Yubico says the most secure plan is two security keys per user (yubico.com).

Standards signal, not a legal duty

NIST classifies the use of the public switched telephone network (PSTN) for out-of-band authentication as the single restricted authenticator at publication (pages.nist.gov). For restricted authenticators, the standard requires the credential service provider to offer subscribers at least one alternative authenticator that is not restricted (pages.nist.gov), and Sec. 3.1.3.3 says verifiers should consider risk indicators such as device swap, SIM change and number porting before using the PSTN to deliver a secret (pages.nist.gov). The final publication is dated **31 July 2025** (csrc.nist.gov). For a small business, the useful reading is that the authors expect phone codes to be one option among several.

Table 3 below compares the three options against the criteria that matter for the decision, including the category of product the publisher offers.

Option	Best for	Main limit	Who receives the code	Backup needed
A. Shared business number (a flat-rate number with an auto attendant that rings team mobiles, such as the publisher's own product described above)	Accounts whose help page accepts the line type and where the delivery test ends in a live person	Menus, after-hours messages and voicemail can intercept automated calls; line-type classification must be confirmed with the provider	Whoever answers the menu route or reads the voicemail, which is not a single named person	Yes: a named mobile and a non-phone recovery email

Option	Best for	Main limit	Who receives the code	Backup needed
B. Carrier mobile held by a named person	Banks, payroll, hiring platforms and any account that accepts only mobile numbers	Depends on one person; lost when they leave or lose the phone	One accountable person	Yes: a deputy's mobile
C. Authenticator app, passkey or security key	Email, domain registrar, payment processor, ad accounts, accounting	Needs enrolment on a device or key; recovery must be planned	The holder of the key or device; no phone number involved	Yes: backup codes offline and a second key

Table 3 makes a plain point: a number optimized for routing inbound calls to a team fits the outward-facing job and fits the credential-recovery job poorly. That is a design observation, not a defect, and no verification behavior of the publisher's product is asserted here.

Recovery, Ported Numbers and Departing Staff

Recovery is where a phone-based choice is tested. When the number is lost, ported or left behind by an employee, each platform's path differs in speed and effort.

When the number is lost or changed

Documented paths vary widely:

- **Google:** backup codes are for when a user loses a phone or changes a number (support.google.com).
- **Microsoft:** after security information is replaced, the user must wait **30 days** before signing in (support.microsoft.com).
- **Apple:** recovery might take several days or longer (support.apple.com).
- **Stripe:** the easiest route is a backup code (support.stripe.com); without one, an owner files a request and the decision may take up to a couple of business days (support.stripe.com), with an approval link valid for 48 hours (support.stripe.com).
- **Gusto:** the old phone is not needed (support.gusto.com).
- **Intuit:** turning off two-step verification without the old number requires government identification or a notarized document (quickbooks.intuit.com).
- **PayPal:** after a number change, codes still go to the old number until it is updated (www.paypal.com).

For a Google Workspace super administrator, a locked-out account may need another super admin or Google Support to reset the password (support.google.com), and Google advises that admins enroll more than one security key (support.google.com). The Canadian Centre says an organization needs a clear recovery plan for lost or compromised factors (cyber.gc.ca).

When the number is ported

A number port changes who controls the line, and it can change how the line is classified (www.bandwidth.com). Re-verify every account first: confirm that each worksheet row still passes its delivery test on the new arrangement before the old service ends. The publisher's guidance on the paperwork is in its letter of authorization article. In the United States, the FCC adopted wireless-carrier rules on SIM changes and port-outs that include an account lock option (www.federalregister.gov). The Federal Register notice gives an effective date of **January 8, 2024**, except for revisions with information-collection requirements (www.federalregister.gov), and an FCC bureau order says compliance is not required until the Office of Management and Budget completes its review (docs.fcc.gov). This report did not locate the later notice announcing a compliance date, so the current status should be confirmed with the carrier. Do not assume the account-lock option is available on any given line until the carrier confirms it. The FCC's consumer page notes that banks, businesses and payment services often use texts to verify identity (www.fcc.gov).

When a person leaves

If the verification phone is a person's mobile, their departure is a recovery event: update each account before their access ends, using the worksheet's owner and deputy columns. The call routing permissions article covers who can see and change a number's routing, which belongs on the offboarding list. The FTC advises, for a hacked email account, making sure the email address and phone number listed are correct (consumer.ftc.gov); the same check belongs in every handover.

Data Analysis and Evidence

The quantitative evidence on phone-based verification comes from four originators: Google, Microsoft, the FIDO Alliance and NIST, plus timing figures in platform help pages. No independent benchmark compares business numbers against personal mobiles for code delivery, and none was found.

Effectiveness figures

Google's May 2019 study, conducted with New York University and the University of California, San Diego, reported that an SMS code to a recovery phone blocked **100%** of automated bots, **96%** of bulk phishing attacks and **76%** of targeted attacks (security.googleblog.com). On-device prompts blocked 100%, 99% and 90% respectively (security.googleblog.com), and users who relied exclusively on security keys had zero targeted-phishing victims in the study (security.googleblog.com). The same experiment reported that **38%** of users did not have access to their phone when challenged (security.googleblog.com), a figure that bears directly on lockout risk for any phone-dependent method.

Microsoft's own pages differ: a 2019 security blog says multi-factor authentication can block over 99.9 percent of account compromise attacks (www.microsoft.com), while a Microsoft Learn page says more than 99.2% (learn.microsoft.com). A 2023 Microsoft Research paper reports a **99.22%** risk reduction across the entire population (www.microsoft.com) and concludes that dedicated authenticator applications outperform SMS-based authentication (www.microsoft.com). The 99.2% figure appears to derive from that research and the 99.9% figure from the older blog, so the two look like different measurements rather than one contradicted claim; the sources do not reconcile them explicitly.

FIDO Alliance's 2025 consumer survey found that **69%** of consumers reported enabling passkeys on at least one account (fidoalliance.org), in a sample of 1,389 adults across several countries (fidoalliance.org). It is an industry-association survey, so it indicates adoption, not security effect.

Timing figures worth planning around

- **Code validity:** NIST says issued recovery codes sent by text or voice are valid for **10 minutes** (pages.nist.gov).
- **Retry intervals:** Indeed advises retrying after ten minutes, then after 24 hours (www.indeed.com).
- **New number trust:** Google says a newly added 2-Step Verification phone can take up to **7 days** to be trusted (support.google.com).
- **Recovery waits:** Microsoft cites **30 days**; Stripe, a couple of business days (support.stripe.com).
- **Backup code counts:** Google issues sets of **10** (support.google.com); Facebook offers 10 recovery login codes (www.facebook.com).

Reading the evidence

A phone-delivered code beats no second step; CISA says any MFA is better than none (www.cisa.gov), yet it also describes text or email codes as the weakest protection among the methods it ranks (www.cisa.gov). The Canadian Centre advises SMS codes only for low-risk logins (cyber.gc.ca), and Google and the FTC each describe text-based verification as exposed to phone-number-based attacks (support.google.com) (consumer.ftc.gov). The numbers support a ranking, not a ban: phone codes suit low-stakes accounts or cases with no alternative, and are weaker than the alternatives for payment, domain and email accounts.

Case Studies and Real-World Examples

(Hypothetical Example) An eight-person electrical contractor

A contractor with eight employees ports its main line to a number with a three-option menu. The owner, Dana, plans to use that number as the verification phone for everything. The worksheet changes the plan.

Dana runs the delivery test. Step 1 fails because the number handles calls only. The voice test reaches a greeting and a menu, and the after-hours test ends in a closed message and a voicemail that two office staff can read. Three of the six tests end in a menu, closed message or voicemail rather than a live person.

The worksheet is then filled out account by account:

- **Email and domain registrar:** passkeys on two security keys, one held by Dana and one by the office manager, plus offline backup codes. No phone.
- **Bank and payroll:** Dana's carrier mobile as the verification phone, the office manager's mobile as the deputy number, after asking each institution which line types it accepts.
- **Payment processor and accounting:** authenticator app, with backup codes printed and stored in the office safe.
- **Google Business Profile:** verification attempted from a device and number a person answers, because Google says IVR systems will not get the code (support.google.com).

- **Hiring platform:** Dana's carrier mobile, since the platform's help says non-fixed VoIP numbers are not allowed.

The business number stays public, keeps its menu and appears in no recovery field. The example is illustrative only and describes no real company.

Implications and Future Directions

Three trends are visible in the first-party sources opened for this report, none of which can be called settled.

First, platforms are moving off SMS. Microsoft's page says it will start phasing out SMS as a method of authentication and account recovery for personal accounts (support.microsoft.com), and Shopify says SMS can no longer be set up as a new two-step method (help.shopify.com). If that direction continues, a business number's role in verification will shrink, and the worksheet's phone columns will become the exception rather than the rule.

Second, standards bodies treat PSTN delivery as restricted and exclude out-of-band codes from phishing resistance: NIST says out-of-band authentication is not phishing-resistant (pages.nist.gov). It also encourages at least two separate means of authentication (pages.nist.gov) and treats changing a pre-registered telephone number as binding a new authenticator (pages.nist.gov), so a phone-number change is a security event in its own right.

Third, recovery is moving toward offline artefacts. NIST describes saved recovery codes as intended to be maintained offline (pages.nist.gov), Shopify's codes work when other methods are unavailable (help.shopify.com), and Etsy points to backup codes when a number is not accessible (help.etsy.com).

Two uncertainties remain. Most cited pages carry no revision date, so each Table 2 row should be re-read before enrolment. And no Canadian regulatory source was reviewed, so Canadian owners should confirm carrier-side protections with their carrier.

Frequently Asked Questions (FAQs)

Can a business use a VoIP number for two-factor authentication?

It depends on the platform and the VoIP type. Microsoft's help page on Microsoft account verification (support.microsoft.com), OpenAI and Upwork say VoIP numbers are not accepted (help.openai.com) (support.upwork.com); Indeed rejects non-fixed VoIP only; Google's verification-error page does not mention VoIP (support.google.com). Check each page and ask the provider which type the number is.

Which accounts should use a business phone number for 2FA?

Few. The worksheet defaults to an authenticator app, passkey or key for email, domain, payments, advertising and accounting, and a named person's carrier mobile where a phone is required. The business number fits only where the help page accepts the line type and the delivery test ends in a live person.

What is the difference between a VoIP and a mobile number for SMS verification?

A mobile number is carrier-issued and generally receives SMS. Fixed VoIP is tied to a physical device; non-fixed VoIP is obtained online without one. Some platforms accept only mobile numbers.

Why do some sites reject VoIP numbers?

Published reasons are thin. Lookup vendors describe screening by number type at signup (developers.telnyx.com), and Indeed states its rule without a reason. Its advice to ask the carrier about line type (www.indeed.com) suggests classification can also be the issue.

Should a business owner's account recovery phone be the business number?

Generally no. Google recommends a mobile that belongs only to the user (support.google.com), and Facebook says the two-factor number cannot also reset the password (www.facebook.com).

Can a business phone number receive SMS verification codes?

Only if it supports text. Landlines generally cannot receive SMS, and Twilio Verify returns an error when SMS goes to a number that does not support it (www.twilio.com). Ask the provider and run step 1 of the delivery test.

Is SMS or an authenticator app better for business accounts?

An authenticator app, in the sources reviewed: Microsoft Research found such apps outperform SMS (www.microsoft.com), Google rates its Authenticator app more secure than SMS (support.google.com), and CISA ranks text or email codes weakest (www.cisa.gov).

What are the risks of a shared business number for two-factor authentication?

The code goes to whoever answers or reads the voicemail, not one accountable person. NIST expects users to maintain their own authenticators (pages.nist.gov), and Canadian guidance advises minimizing shared accounts (www.cyber.gc.ca).

What happens if a business loses access to its 2FA phone number?

Use a backup code if one was saved (support.google.com). Without one, platforms run recovery processes with waits, such as 30 days at Microsoft or a couple of business days at Stripe (support.stripe.com).

Conclusion

A business phone number is a good public contact point and, in most cases, a mediocre verification phone. The evidence assembled here points to a simple division of labor. Platforms differ on line types, so a rule must come from each platform's own help page, not from a rule of thumb. Delivery differs from acceptance, so the number must pass a delivery test that includes its menu, its voicemail and its after-hours behavior. Accountability differs from convenience, so a named person with a deputy should receive any phone-based code.

The worksheet in Table 2 applies this: fill each row from the platform's page, run the six-step test, choose among the business number, a named mobile and no phone, and record the owner and backup. Rows without a first-party statement stay "ask/verify". Authenticator apps, passkeys and security keys are the default for the accounts that matter most, in line with NIST, CISA and the Canadian Centre for Cyber Security, none of which imposes a legal duty on a private business.

Before the next port or the next departure, re-verify every account, store backup codes offline and keep a non-phone recovery email. Where a platform insists on a phone, the owner's carrier mobile is the safer recipient.

Source links

Links cited in this article, in order of first appearance. Full addresses are provided for readers using extracted text.

1. https://support.microsoft.com/account-billing/troubleshooting-verification-code-issues-409090c4-92b5-42b9-8ae6-bcc97e62fc48
2. https://help.openai.com/en/articles/8983024
3. https://support.upwork.com/hc/en-us/articles/33076260715923
4. https://support.google.com/mail/answer/114129
5. https://support.google.com/business/answer/7107242?hl=en
6. https://help.twilio.com/articles/4404317129627-Troubleshooting-Undelivered-Verify-and-Authy-SMS-Messages
7. https://pages.nist.gov/800-63-4/sp800-63b.html
8. https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html?m=1
9. https://www.twilio.com/docs/lookup/v2-api/line-type-intelligence
10. https://www.bandwidth.com/support/en/articles/12823347-phone-number-lookup-faq
11. https://www.fcc.gov/general/voice-over-internet-protocol-voip
12. https://go.paychex.com/sites/default/files/2026-10/Oasis_MFA_Guide.pdf
13. https://kdp.amazon.com/en_US/help/topic/G6HTFZJLJ7AJQ56R
14. https://faq.whatsapp.com/684051319521343
15. https://developers.telnyx.com/docs/identity/number-lookup/index
16. https://www.indeed.com/help/job-seekers/articles/34540805299085-phone-verification-issues-basic-troubleshooting
17. https://developers.sinch.com/docs/number-lookup-api-v2/overview
18. https://old-support.plivo.com/hc/en-us/articles/360049279691-FAQ-Number-Lookup-API
19. https://support.google.com/accounts/answer/185839
20. https://www.twilio.com/docs/verify/authentication-channels
21. https://squareup.com/help/us/en/article/5593-2-step-verification
22. https://quickbooks.intuit.com/learn-support/en-us/help-article/security-risk/verify-account-multi-factor-authentication/L2Xp0GNiT_US_en_US
23. https://www.facebook.com/help/147926301947841
24. https://support.google.com/accounts/answer/185834
25. https://faq.whatsapp.com/1120385166078156

26. https://faq.whatsapp.com/1344487902959714
27. https://support.google.com/accounts/answer/183723
28. https://support.google.com/accounts/answer/13548313?hl=en
29. https://support.google.com/accounts/answer/1187538
30. https://www.godaddy.com/help/enable-an-identity-verification-method-for-your-godaddy-account-42665
31. https://www.namecheap.com/support/knowledgebase/article.aspx/10073/45/how-can-i-use-the-totp-method-for-twofactor-authentication
32. https://developers.cloudflare.com/fundamentals/user-profiles/2fa
33. https://www.rbcroyalbank.com/ways-to-bank/mobile/rbc-mobile-app/2step
34. https://www.wellsfargo.com/privacy-security/fraud/articles/two-factor-authentication
35. https://www.wellsfargo.com/help/online-banking/advanced-access-faqs
36. https://support.gusto.com/article/106622317100000/set-up-manage-and-troubleshoot-2-step-verification
37. https://support.stripe.com/questions/enable-two-step-authentication
38. https://www.paypal.com/us/cshelp/article/what-is-2-step-verification-help167
39. https://support.google.com/google-ads/answer/12864186?hl=en
40. https://www.facebook.com/business/help/216940652189296
41. https://www.facebook.com/help/458801388097062
42. https://www.facebook.com/help/148233965247823
43. https://central.xero.com/0/article/Set-up-multi-factor-authentication
44. https://help.etsy.com/hc/en-us/articles/115015569567-How-to-Make-Your-Account-More-Secure
45. https://help.shopify.com/en/manual/your-account/logging-in/two-step-authentication/sms
46. https://www.cyber.gc.ca/en/guidance/baseline-cyber-security-controls-small-and-medium-organizations
47. https://cyber.gc.ca/en/guidance/cyber-security-privacy-risk-management/itsp10033/access-control
48. https://support.apple.com/122621
49. https://cyber.gc.ca/en/guidance/steps-effectively-deploying-multi-factor-authentication-mfa-itsap00105
50. https://fidoalliance.org/passkeys
51. https://cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf
52. https://www.cisa.gov/require-multifactor-authentication
53. https://www.ftc.gov/business-guidance/small-businesses/cybersecurity
54. https://cyber.gc.ca/en/guidance/secure-your-accounts-and-devices-multi-factor-authentication-itsap30030
55. https://www.ncsc.gov.uk/collection/small-organisations-guide-to-cyber-security/secure-your-important-online-accounts
56. https://bitwarden.com/help/two-step-recovery-code
57. https://yubico.com/blog/backup-recovery-plan
58. https://csrc.nist.gov/pubs/sp/800/63/b/4/final
59. https://support.apple.com/118574
60. https://support.stripe.com/questions/sign-in-to-your-stripe-account-without-a-2fa-device-and-or-backup-code
61. https://support.stripe.com/questions/sign-in-to-your-stripe-account-without-a-two-step-authentication-device-or-backup-code

62. https://www.paypal.com/us/cshelp/article/what-can-i-do-if-ive-changed-my-mobile-number-and-cant-log-in-help678
63. https://support.google.com/a/answer/9436964?hl=en
64. https://support.google.com/a/answer/9011373
65. https://www.federalregister.gov/documents/2023/12/08/2023-26338/protecting-consumers-from-sim-swap-and-port-out-fraud
66. https://docs.fcc.gov/public/attachments/DA-24-649A1.pdf
67. https://www.fcc.gov/cell-phone-fraud
68. https://consumer.ftc.gov/node/86584
69. https://www.microsoft.com/en-us/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks
70. https://learn.microsoft.com/en-us/entra/identity/authentication/concept-mandatory-multifactor-authentication
71. https://www.microsoft.com/en-us/research/publication/how-effective-is-multifactor-authentication-at-deterring-cyberattacks
72. https://fidoalliance.org/fido-alliance-champions-widespread-passkey-adoption-and-a-passwordless-future-on-world-passkey-day-2025
73. https://consumer.ftc.gov/node/76732
74. https://help.shopify.com/en/manual/your-account/logging-in/two-step-authentication/recovery-codes
75. https://help.etsy.com/hc/en-us/articles/31554318019863-How-to-Update-the-Phone-Number-in-Your-Etsy-Account
76. https://www.twilio.com/docs/api/errors/60205

THE PUBLISHER

About Auto Attendant

Auto Attendant gives a small business one phone number and a recorded menu that sends each caller to the right person. The call rings the mobile that person already carries, using their normal dialler and their normal mobile plan. Pricing is a single flat monthly fee for the whole company rather than a charge for each user, and there is no app, desk phone or hardware to install.

One number, one menu, the phones you already own

A caller dials the business number, hears a short greeting and chooses an option. Each option can ring one mobile, ring several at once so whoever is free answers first, or try people one after another in a set order. There is no limit on how many people sit on the receiving end, because nobody is billed per seat. Setup is done by the owner in a few minutes: pick a number, write the greeting, and point each option at a mobile.

What it deliberately is not

An auto attendant routes a call; it does not answer one. Nobody at Auto Attendant speaks to callers, and no AI stands in for a receptionist. A business that wants its calls handled, messages taken and appointments booked wants an answering service, which is a different product at a different price. A business that needs call recording, queues, agent dashboards or CRM integration wants a contact centre platform. Auto Attendant is for the case where the call should simply reach the right pocket.

Keeping personal numbers off the internet

The business number is the only number a caller ever sees. Personal mobile numbers are never displayed and never given out, which is what lets an owner put a number on a website, an invoice, a van or a Google Business Profile without handing a personal line to everyone who finds it. An existing advertised number can be ported across and kept, and the old line keeps working while the port is in progress.

Work with Auto Attendant

Visit Auto Attendant to see how it works, how it compares to a personal mobile, Google Voice and a full phone platform, and the current pricing.

Telephone number portability, emergency calling and caller-ID rules differ by country and change over time. Articles published here describe general practice and cite primary regulator and carrier sources; they are not a guarantee of any timeline, and they are not legal or regulatory advice for a specific business.

Website: https://autoattendant.io

This article is educational. Verify consequential medical, legal, financial, regulatory and technical decisions with appropriate professionals and the cited primary sources. Company services are described separately from the article's research findings.