Robokiller Enterprise

6 Ways to Protect Your Team Against Text Scams

How to proactively solve today’s most pressing communications threat.

Table of Contents

Introduction

The extent of the text scam problem

How scammers target your employees via smishing

Watch out for these common text scams

Why the text scam problem is a must-solve

How to protect your team from phone scams

Step #1: Recognize the red flags

Step #2 Keep information private

Step #3: Stop, think, and verify

Step #4: Block and report scam attempts

Step #5: Train your employees on anti-scam protocols

Step #6: Protect your team with Robokiller Enterprise

Introduction

Scammers are out to disrupt your business and steal your assets — and text messages are their preferred way of going about it. Fortunately, with the right education and preparation, you can keep your organization safe from harm.

In this eBook, we'll detail 6 ways to protect your team against text scams. These tips, supplemented with a dedicated robotext protection service, will position you to keep your company scam-free.

Susan - CEO
Can you send me those financials when you get a chance?

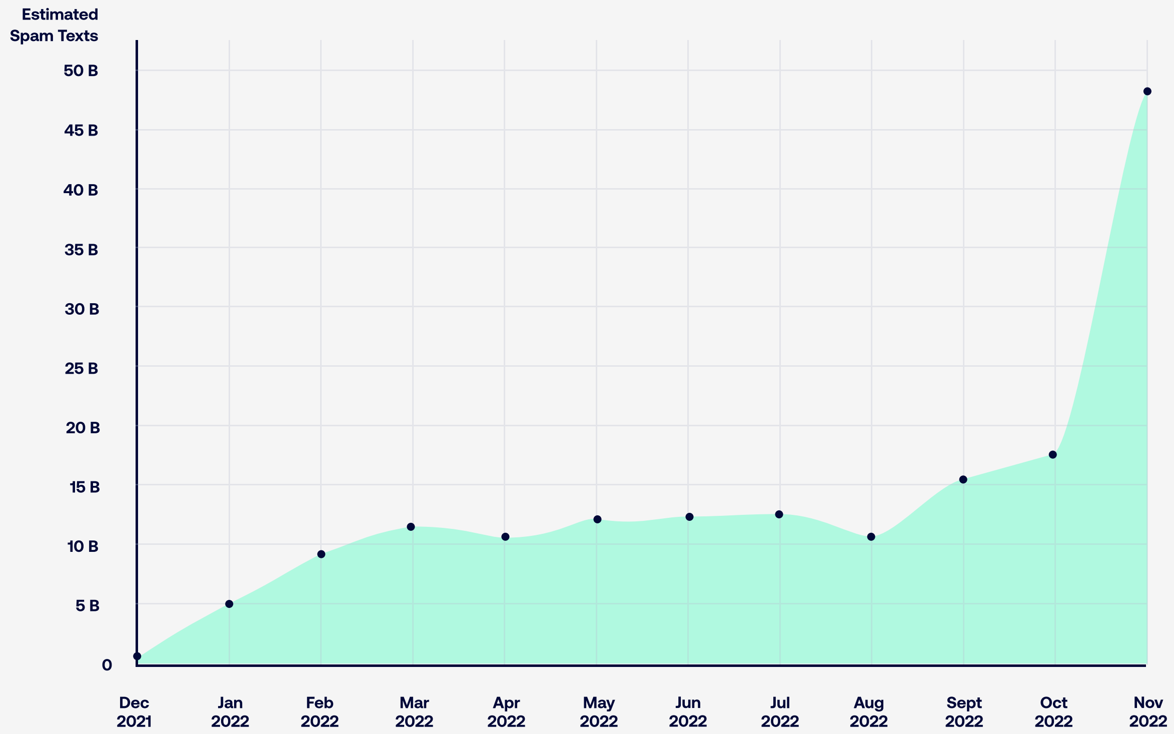
The extent of the text scam problem

Phone scams have plagued our phones since they were attached to the wall with a cord. Unfortunately, as technology has advanced, so have scammers' tactics. Scam texts are the new scam call, and they're as dangerous as ever.

Many spam and scam texts are deployed as part of smishing schemes — a type of phishing attack that uses SMS as the medium. However, the same principles can be extrapolated to social media apps, email, or any other platform that supports messaging.

In 2021, smishing attacks increased by 69% globally and by 24% in the United States. According to the Federal Trade Commission (FTC), the average scam costs the victim $1,500. And per Robokiller estimates, unwanted texts are infiltrating people's phones at never-before-seen levels.

Estimated Spam Texts Per Month, United States



How scammers target your employees via smishing

The goal of smishing scams is to gain access to sensitive information. Scammers may target all kinds of confidential data, from phone numbers and passwords to bank account and credit card details. Once they get what they need, they can use it to infiltrate and sabotage their target.

Smishing attacks generally include a link that directs the recipient to a phony website, which may convincingly resemble the company or entity it's impersonating. The success of the scam depends on the target following the link and unwittingly handing over their confidential details to the scammer. In other cases, simply clicking the link can download harmful malware to the victim's device, which the scammer may then use to control the affected phone, computer, or tablet.

In addition to smishing, there are more specific, focused forms of phishing. Spear phishing, for example, is a phishing attack that targets a specific person or group within a business. Whaling occurs when the scammer targets a CEO, spokesperson, or other powerful individual in an attempt to get the biggest possible return out of the scam.

> Ultimately, whether the target is an entry-level employee or the founder of the company, a successful smishing attack can yield devastating consequences. Recognizing scams in action can help you avoid disaster.

Watch out for these common text scams

The element of surprise is a crucial aspect of any text scam; when you remove it, you're much better equipped to identify when you're being targeted and escape the situation unscathed. Given that most employees use their personal smartphones for work, these common robotext scams are especially important for your team to avoid:

Apple ID scams: An employee might get a text that seems like it's from the App Store, Apple Pay, or another sect under the Apple umbrella claiming that their Apple ID was involved in a purchase or was potentially compromised. The message might prompt them to follow a link and enter information. If scammers get their hands on the recipient's Apple ID, they get access to everything in their cloud.

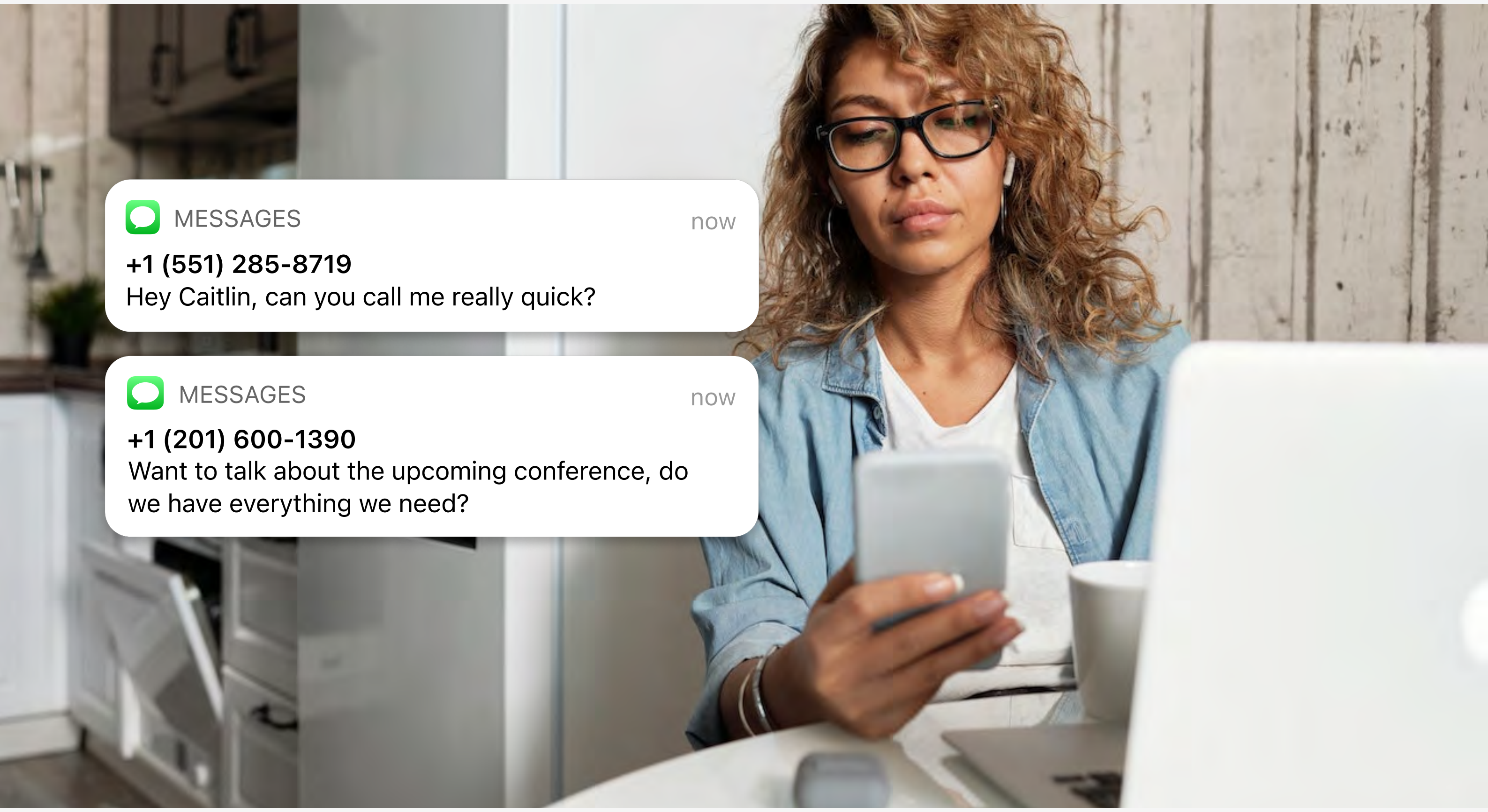
Bank scams: Similarly, scammers might pretend to represent a bank or financial institution and claim that there's a security problem with a business account. However, it's only after someone clicks the link and inputs their credentials that the security problem will occur.

Delivery scams: Delivery scams aim to take advantage of people's anticipation when waiting on a package. These scam texts may come in the form of phony tracking updates or fake delivery confirmation links.

Government agency scams: The most intimidating text scams are those that appear to come from government agencies like the IRS. These scams generally accuse the recipient of owing some outstanding balance or require them to take action to avoid facing serious consequences. Remember: If government agencies need something, they won't reach out by text message.

In addition, train your employees to stay on the lookout for impersonation scams that appear to be from you or another supervisor.

Scammers know that there's pressure to respond quickly when the boss reaches out. They utilize this to their advantage by making requests — for instance, they might send a text asking the recipient to share a spreadsheet with client information or initiate a wire transfer.



MESSAGES now
+1 (551) 285-8719
Hey Caitlin, can you call me really quick?

MESSAGES now
+1 (201) 600-1390
Want to talk about the upcoming conference, do we have everything we need?

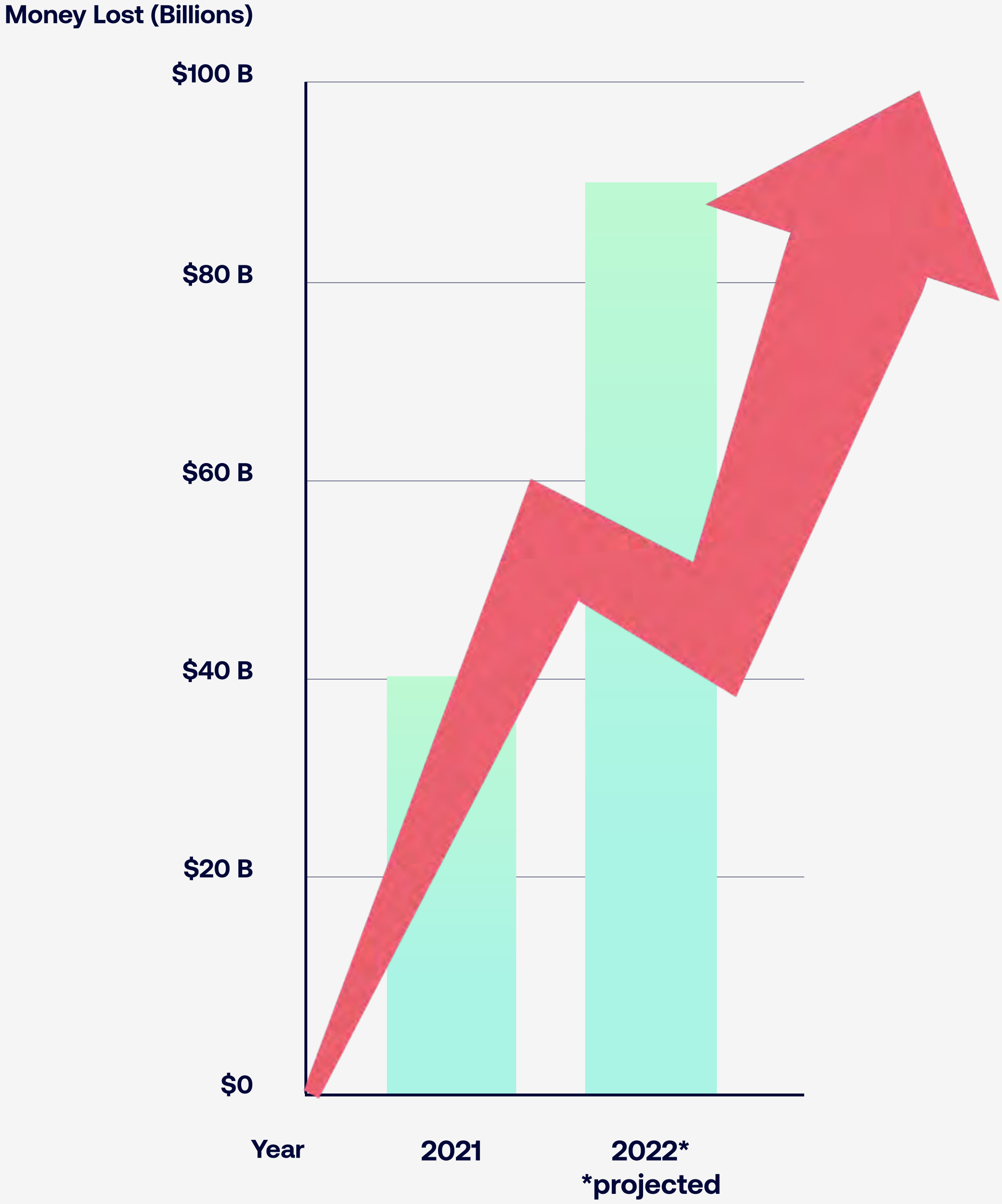
Typically, the initial text will seem innocuous. The scammer might reach out with something along the lines of, "It's your boss — I'm stuck in a meeting but let me know if you get this message." Once the employee responds, the scammer knows it's an active number and will proceed with the scam.

> If your employees receive messages like these, tell them to treat them with skepticism and reach out to you through a known channel to verify the request.

Why the text scam problem is a must-solve

Spammers have been annoying people since the dawn of telemarketing, but today's scams are more elaborate, effective, and dangerous than ever before. Look no further than the fact that scammers more than doubled their stolen profits in 2022 compared to 2021.

Money Lost to Phone Scams



When scammers target businesses, they know they're eyeing a much bigger jackpot — if sensitive business information falls into the wrong hands, disaster could ensue. Business owners who have fallen victim to text scams may experience:

- **Damaged or lost property**
- **Drained bank accounts**
- **Identity theft and/or sabotage**
- **Lost intellectual property**

> These dangers are amplified by the fact that 2022 saw about 26% of employees in the United States working remotely. Chances are, that trend isn't going to reverse itself. That means that while employers once kept their tech in-house, more than a quarter of employees are now using their personal and/or work devices out-of-office.

Unfortunately, this makes it more difficult to monitor usage and enforce safety protocols, leaving businesses more susceptible to scams. The good news, however, is that there are steps you can take to empower your team to thwart the scammers and keep your organization safe.

Robokiller Enterprise

How to protect your team from phone scams

Scammers impact productivity and put your business at risk, but there are ways you and your team can stay a step ahead of them.

Book a demo

Step #1: Recognize the red flags

In order to stay ahead of scammers, it's imperative to think like them. Fortunately, most of them tend to think in similar ways. Text message scams often include many of the same features, which can become glaring red flags when you know what to look for.

Encourage your team to be wary of text messages that…

- **Include unusual characters:** Scammers sometimes use strange (non-native to the language) characters in the body of their texts or even in the addresses they use to send the messages (e.g., Å, ÿ, ñ, Ø).

- **Prompt you to follow a link:** A legitimate business or government agency generally won't include links in their text messages, especially if you're not already in communication with them. One exception: If you're in the middle of verifying an account, resolving an open issue, or otherwise in active communication, a text message containing a link may be warranted.

- **Create a sense of urgency:** Scammers like to create an "urgent" situation to get you to act fast, before you notice you're being scammed. If the situation was really so time-sensitive, the people on the other side probably wouldn't be reaching out via text.

- **Use threatening or intimidating language:** One especially despicable way scammers create that fake urgency is by attempting to threaten or intimidate their targets. They may claim that failing to take action could result in serious consequences like lost services, fines, or even jail time.

- **Request odd payment methods:** If you're ever asked to transfer money via an unusual and/or oddly specific payment method (like a Best Buy gift card), you can all but guarantee that it's a scammer on the other end.

When you and your team are able to recognize these common signs of text message scams, you'll be in a better position as a company to avoid financial loss.

Step #2: Keep information private

Scammers don't necessarily choose their targets at random; in many cases, they find (or purchase) contact information online. While there's nothing most people can do about big data breaches that cause this information to get out, there are steps your employees can take to fortify your company's privacy.

To avoid being on the lists that scammers pick up, remind them to refrain from giving out any kind of potentially sensitive information online. Many people plug in their phone numbers, addresses, and contact information without thinking twice when signing up for social media accounts, making online purchases, or even calling toll-free numbers.

Step #3: Stop, think, and verify

Scammers want people to act before they have a chance to think, and some may even show signs of frustration when someone asks perfectly reasonable questions. That's because the success of the scam depends on their ability to shake up the target and convince them to take action before they see the situation for what it is.

While there are, of course, actual urgent situations, a legitimate professional won't get upset about inquiries. Even more tellingly, it's unlikely they would contact someone through text message in the first place. It's important to take the time to verify the sender by contacting them at a number or email address that's know to be legitimate.

+1 (551) 285-8719
Hey, it's your boss. Stuck in a meeting - send me the new account. Thanks.

Step #4: Block and report scam attempts

You can help protect your own business as well as others by blocking and reporting the scam texts that come your way. When you get a text message that you recognize as spam, block the sender immediately and forward the message to SPAM (7726). You can also report it to the FTC online.

It can be tempting to turn the tables when you realize you've been contacted by a scammer, but it's best not to respond. Just by answering the text, it shows the scammer that they've found an active number and encourages them to keep you in their sights. Block and report them to avoid further harassment.

Step #5. Train your employees on anti-scam protocols

The battle against spam and scams is easier for a business to handle when all of its links are up to the task. By giving your employees the tools to succeed, they can help protect themselves and the business itself from text scams.

Here's what you can do:

- **Educate your team:** The more knowledgeable your staff is, the more they can do to help protect the business. Teach them about the dangers of text scams, the red flags to watch out for, and how they should handle a text scam if they encounter one.
- **Clearly define your Bring Your Own Device (BYOD) policies:** If you allow employees to use their personal devices for work purposes, be sure to lay out clear policies for how they're to be used. Have your employees keep their privacy software up to date, use multi-factor authentication, and encrypt their messages, for starters.
- **Ensure proper communication between channels:** Proper communication can be an excellent safeguard against text scams. Remind your employees to verify whom they're talking to — even if the interaction seems legitimate.
- **Keep some information on a need-to-know basis:** You can prevent information from leaking by controlling who has access to it. For sensitive details like account numbers and passwords, consider sharing only with the people in your company who need to know them.

When everyone in your business is on the same page, your walls are much more difficult to break through. However, no amount of education alone can eliminate the possibility of text scams; fortunately, you can bring in reinforcements.

Step #6: Protect your team with Robokiller Enterprise

Preparation and education can go a long way in the war against spam and scams, but the reality is that you can’t win it alone. An efficient and effective scam text blocker like Robokiller Enterprise can take on the heavy lifting and fill in the gaps, allowing your team to focus on moving your business forward.

Robokiller Enterprise empowers companies to defend their team against text scams. Whether you’re a distributed team that needs a way to protect its employees or are seeking ways to seamlessly integrate SMS blocking into company systems, we can help.

To learn more about our 99% effective phone scam protection, contact us today. We’ll be happy to show you how our products can protect your business, no matter your unique needs.

Try it free

Book a demo