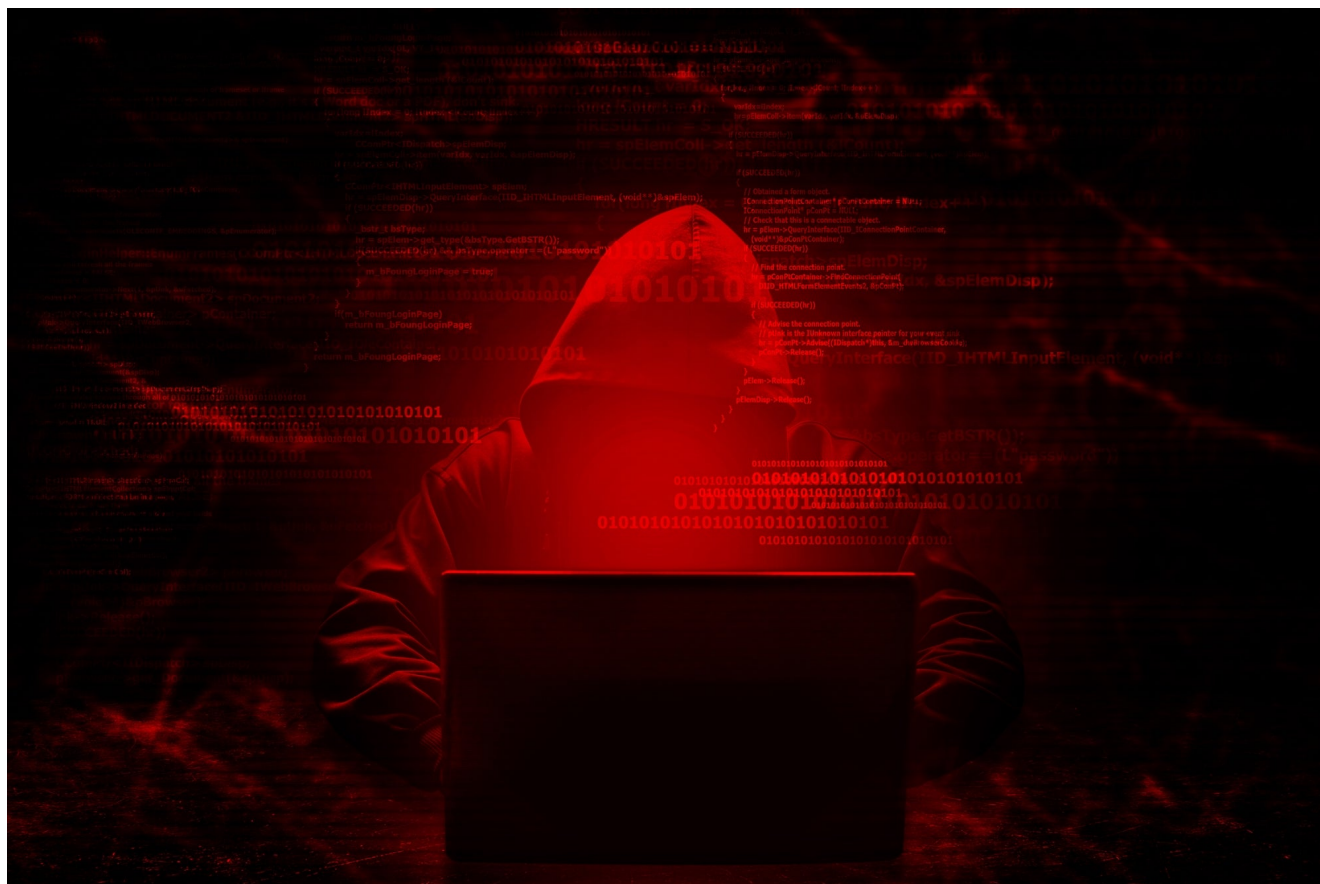


A Scammer Tried to Come For My Small Business – and Yours Could Be Next. Here's How to Protect Yourself.



Opinions expressed by Entrepreneur contributors are their own.

Several months ago, an employee of mine received a text from me saying I was in a meeting and needed her to do a “quick task” and “physically go to any nearby store and purchase an Apple gift certificate. I need the card’s back codes for a presentation. I [will] reimburse you when I’m through. Thanks.”

The employee thought the text seemed “odd” and forwarded it to our management team. She was right; I never sent that text. It was a scam.

We immediately alerted everyone in our growing company to look out for scam texts and to remind our clients, mostly business owners, to be aware.

Related: I'm a Business News Editor, and Even I Fell Victim to an Online Scam That Cost Me \$300

Scams are proliferating

This wasn't the first time an employee received a scam text "from me," and I assumed it wouldn't be the last. I decided to learn more so I could warn my team and our clients about what to look for – before it's too late.

The info was overwhelming and startling. The biggest problem is most small business owners assume (wrongly) their companies are too small for cybercriminals to target. So they don't protect themselves, leaving their businesses as sitting ducks.

But you can protect your small business. Here's some of what I learned.

The 2023 Hiscox Cyber Readiness Report contained some scary stats:

- The number of cyberattacks increased for the fourth consecutive year.
- 53% of businesses suffered at least one cyberattack in the last 12 months.
- The median cost of an attack topped \$16,000. But 21% of companies experiencing a cyberattack said it threatened the viability of their businesses.
- The attack rate grew from 23% to 35% in the last three years for small businesses with fewer than 10 employees.

The rise of text scams

I started there because we were targeted – twice – by a text

scammer. When the pandemic erupted and so many businesses (like ours) had employees scattered nationwide, the number of text scams, many targeting small businesses, spiked and remained elevated.

In 2022, text scams cost businesses \$330 million, more than twice the amount in 2021 and almost five times 2019's losses.

It's critical your team knows what to look for. In addition to being alert to unusual messages, like the one my employee received, the top business text scams share several common characteristics. Scammers often:

- Masquerade as a trusted entity mimicking government agencies and companies like FedEx, Amazon and Google.
- Create a sense of urgency by pushing for quick decisions before their claims can be verified.
- Threaten dire consequences unless immediate payment is made.
- Request payment via untraceable payment methods like wire transfers, reloadable cards or gift cards, making it nearly impossible to reverse or track transactions.

According to the FBI, Business Email Compromise (BEC) scams have led to more financial losses than any other fraud in the U.S. BEC scammers generally target the business owner, CFO or accounting department, asking for money to be wired to them for what sounds like legitimate reasons.

Related: Why Do We Let Ourselves Get Scammed?

Phishing around

Phishing scams try to trick people into revealing personal information or click on malicious links. Phishing attacks are often disguised as legitimate companies' emails, texts or social posts. However, the messages' links lead to fake websites that steal your information (BECs are one form of

phishing).

Phishing is a huge concern. APWG's 2022 Phishing Activity Trends Report shows over 4.7 million attacks in 2022, representing 150% annual growth since 2019.

After my research, we immediately instituted protection measures. Scammers often target multiple employees simultaneously, so we encourage our staff to share information about texts, emails or other messages that seem suspect.

Plus, before responding to a message from anyone on staff asking for money or credit card information, they should first check with the person who made the ask. Managers were told not to make legitimate asks via these channels to avoid confusion.

How to avoid getting scammed

Tell your employees to:

- Never click on links in suspicious emails or texts or open attachments from unknown senders.
- Always check the sender's email address. Phishing emails often have misspelled or spoofed email addresses.
- Hover over links before clicking on them to see where they lead.
- Be careful about what information they share online.
- Be suspicious of any unsolicited requests for personal information

We also distributed a scam-spotting brochure we got for free from the FTC.

Related: Social Media Fraud Is On the Rise – And Even the Most Savvy Are Getting Scammed. Here Are the Most Common.

Ransomware is everywhere

Verizon's 2023 Data Breach Investigations Report says about 24% of cyber breaches are ransomware attacks. It's hard to avoid ransomware – Verizon says it's ubiquitous in businesses of all sizes and all industries.

To protect your business from ransomware demands:

- Regularly backup all critical business data and store it securely offline or in the cloud. If compromised, you can restore your data without paying the ransom.
- Ensure all operating systems, applications and software are updated with the latest security patches.
- Install a robust antivirus and anti-malware program on employees' computers.
- Implement a password policy where employees must use and change unique passwords every 90 days.
- Enable firewalls on all devices and networks.
- If you do get attacked, immediately turn off all automatic backups.
- Invest in cybersecurity. According to the Hiscox report, small businesses now spend a median of \$8,100.

The most essential element is to educate your employees. Verizon's report says 74% of all breaches involve the human element.

Verizon says, "Cybercriminals are coming for [your] data." We are lucky our employee didn't act on the text she got and we didn't lose money. Hopefully, if you educate your team about what to look for, your company can avoid becoming the victim of scammers.

<https://www.entrepreneur.com/science-technology/beware-of-online-scams-that-can-hurt-your-small-business/458876>