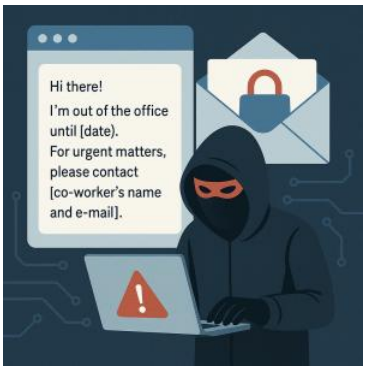
Your Vacation "Auto Reply" Might Be a Hacker's Favorite Email



You set it. You forget it. And just like that, while you're packing for vacation, your inbox starts automatically broadcasting:

"Hi there! I'm out of the office until [date]. For urgent matters, please contact [coworker's name and e-mail]."

Sounds harmless, right? Convenient, even.

Except…that's **exactly** what cybercriminals love to see.

Your auto-reply – the simple message meant to keep things organized and moving smoothly – is also a gold mine of intel for bad actors looking for an easy way in.

Let's break it down. A typical OOO message might include:

- Your name and title
- Dates you're unavailable
- Alternate contacts (with their e-mail addresses)
- Internal team structures
- Even details about *why* you're gone ("I'm at a conference in Chicago…")

This gives cybercriminals two major advantages:

1. **Timing:** They now know you're unavailable and less likely to notice suspicious activity.
2. **Targeting:** They know exactly who to impersonate – and who to target with the scam.

That's the foundation for a perfect phishing or business e-mail compromise (BEC) attack.

How The Scam Usually Plays Out

Step 1: Your auto-reply message is sent.

Step 2: A hacker uses it to impersonate you or the alternate contact you listed.

Step 3: They send an "urgent" e-mail requesting a wire transfer, password or sensitive document.

Step 4: Your coworker, caught off guard, assumes it's legit.

Step 5: You come back from vacation to find out someone sent $45,000 to "a vendor."

This happens more frequently than you might think, and it is even riskier for businesses that travel.

If your company has staff who travel often, especially executives or sales teams, and someone else handles communications while they're away (like a personal assistant or office admin), this creates **prime conditions** for cybercriminals:

- The admin is fielding e-mails from multiple people
- They're used to handling payments, documents or sensitive requests
- They're working fast, trusting the people they *think* they're hearing from

One well-crafted fake e-mail can slip through – and suddenly your business is dealing with a costly breach or fraud incident.

How To Protect Your Business from Auto-Reply Exploits

The solution isn't to ditch OOO replies altogether – it's to **use them wisely** and put safeguards in place. Here are a few suggestions:

1. **Keep It Vague**

Skip the detailed itinerary. Don't list who's covering for you unless it's absolutely necessary.

Example: "I'm currently out of the office and will respond to your message when I return. If you need immediate assistance, please contact our main office at [main contact info]."

2. **Train Your Team**

Make sure your staff knows:

- Never act on urgent requests involving money or sensitive info based on **e-mail alone**
- Always verify unusual requests through a second channel (like a phone call)

3. **Implement E-mail Security Tools**

Utilize advanced e-mail filters, anti-spoofing measures and domain protection to minimize the likelihood of impersonation attacks reaching your inbox.

4. **Use MFA Everywhere**

Multifactor authentication (MFA) should be enabled across all e-mail accounts. Even if a hacker obtains a password, it prevents them from gaining access.

5. **Work With an IT Partner Who Monitors Activity**

A proactive IT and cybersecurity partner can detect login attempts, phishing attacks and abnormal behavior *before* damage is done.

Want To Vacation Without Becoming a Hacker's Next Target?

We help businesses build cybersecurity systems that work – even when your team's out of office.

Click Here To Book A FREE Security Assessment.

We'll check your systems for vulnerabilities and show you how to lock down the risks, so you can actually enjoy that vacation without worrying about your inbox betraying you.

Questions? Call our Glenside, PA office today at 267-699-2551. Or visit us on the web at AOR-ITS.com to learn more about our proven managed IT solutions, including cybersecurity, for small local businesses.