5 Ways to Help Your Employees Identify Email Red Flags

Email scams are getting more sophisticated and harder to spot. Security teams can thwart scammers by teaching employees these common tip-offs.



Key Points

* Most cyberattacks can be traced back to malicious emails.
* Attackers’ latest techniques have made it harder to spot fake emails.
* Developing clear steps to identify and report email scams is critical for businesses to prevent fraud.

[**Phishing**](https://www.mimecast.com/content/what-is-phishing/) has evolved into a sophisticated and widespread problem, ranking as the number one complaint in the [**FBI’s 2022 Internet Crime Report**](https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf). Employees are constantly barraged by phishing emails that carry malicious links or attachments designed to drop malware, steal network credentials, or otherwise damage their company’s business.

In fact, 97% of companies surveyed for Mimecast’s [***State of Email Security 2023***](https://www.mimecast.com/state-of-email-security/) (SOES 2023) say they experience email-based cyberattacks. To block these threats, security teams need to keep their staffs informed and vigilant on current trends and best practices. Otherwise, companies risk data breaches, downtime, and the losses that accompany them.

Security teams need to use every tool at their disposal, from interactive video to [**phishing simulation**](https://www.mimecast.com/content/phishing-simulation/) to basic “how-to” guides.

Identify The Red Flags of Phishing

Some universal rules can help protect business email users and their companies’ data. Here are five lessons for employees:

1. **Carefully Read the Content:** Look for typos and misspellings, especially of official titles or departments, since those mistakes can signify an unfamiliarity with the targeted organization.

2. **Dive into the Details:** Small, important details in a standard email can be overlooked by cyber criminals, like subject phrasing, logo attachments, or signatures.

3. **Look for Suspicious Links and Attachments:** Any link or attachment should be checked before opening, since even a single click can compromise a computer or network.

4. **Think About the Timing:** Emails received after standard business hours may signify an increased likelihood of fraud, like an email from a supervisor sent at 3 a.m.

5. **Trust Your Instincts:**  If an email looks strange, err on the side of caution and check for other red flags, contact the IT team, externally confirm with the sender before continuing — or all of the above.

The Bottom Line

Email is one of the biggest cybersecurity vulnerabilities for businesses, and phishing remains the most common cybercrime reported to the FBI. But security teams can proactively train staff to identify red flags and minimize the risk of business email compromise. By carefully reading emails, remaining cautious of links or attachments, and checking details like timing and standard procedures, employees can avoid falling for common phishing [**email scams**](https://www.mimecast.com/content/phishing-email-scams/) and stay vigilant in keeping their company’s data safe and secure. Learn more about Mimecast’s [**cybersecurity awareness training**](https://www.mimecast.com/products/security-awareness-training/).