

BEWARE THE BILL: HOW TO SPOT A FAKE INVOICE

Scammers are becoming increasingly sophisticated and continuously evolving their attacks to avoid detection. A popular scheme is to pose as a business's vendor, tricking accounts payable departments with invoices for unwanted or even nonexistent goods and services. In 2020, there was a **200% increase in business email compromise (BEC) attacks** focused on invoice or payment fraud.

It may start with an email, phone call or physical bill. The con artist will pretend to be your trusted merchant or a past vendor verifying a purchase. Their goal is to fool or pressure an employee into cutting a real check for a fake charge, which can cost your business hundreds or even thousands of dollars.

5 COMMON FAKE INVOICE SCAMS

Some of these gifts are as old as paper itself. The Federal Trade Commission lists **a few common fake invoice scams**, including:

1. **Directory Listings:** Con artists bill a company for placement in a non-existent online directory or phone book.
2. **The URL Hustle:** A business gets a notice that its website domain is about to expire, which includes the threat that the company will lose its trademarks if a fee isn't paid immediately.
3. **The Charity Con:** An invoice indicating an ad purchase in a fundraising calendar or a guide from a seemingly legit charity (e.g., suffering children) designed to entice an accounts payable manager to pay more quickly.
4. **The Supply Swindle:** A phony vendor invoices for anything from printer toner to cleaning chemicals. Sometimes a "free" sample is mailed, and if the company doesn't send it back in a timely manner, the scammer

sends a follow-up letter insinuating the company has agreed to purchase said products.

5. **The Check Cheat:** A business gets a check from an unknown entity purporting to be a company, government agency or nonprofit. If the check is cashed, a contract is generated stating the business has now signed up for a recurring service it neither needs nor wants.

Regarding the last two scams, in particular, it's worth noting that [federal law](#) prohibits the solicitation of goods and services masquerading as an invoice.

AVOIDING FAKE INVOICES

How can you spot a fake invoice? While they are often presented on convincing letterhead with a realistic corporate logo, fake invoices typically include urgent or threatening language (e.g., 90 days past due) to inspire an employee to pay quickly – before the scheme can be detected.

The hardest-working scammers know your address, your suppliers and the boss's name, so you must be vigilant to prevent this kind of fraud. Follow these tips to avoid getting hoodwinked by a fraudulent bill:

- **Train employees to be wary.** Cross-check orders with invoices. Match account numbers to ensure a vendor is legit. Beware of companies that don't provide a phone number.
- **Don't open invoice attachments from unknown senders.** They might contain malware or ransomware – and then you have a whole new host of problems.
- **Establish purchasing responsibility** by limiting the number of employees authorized to place orders or pay invoices.
- **Create and review purchasing procedures** to prevent an unexpected call, email, or invoice from triggering an expensive mistake.
- **Check all invoices closely.** Make sure all supplies on the invoice were ordered and delivered.
- **Keep in mind** that if you receive merchandise you didn't order, you are not required to pay for it.

If you suspect you've been the victim of a scam, you have options. Contact the [U.S. Postal Inspection Service](#) or the [FTC](#), and notify your local [Better Business Bureau](#) (BBB).