# 5 slippery small business scams and how to avoid them

When governments stepped up to help insulate small businesses from the financial calamities of COVID-19, fraudsters took it as their cue to cash in. More than 47% of companies worldwide reportedly experienced fraud in the past 24 months, costing a jaw-dropping $42 billion in collective losses, according to PwC's Global Economic Crime and Fraud Survey 2020.

Knowing how to spot potential scams is the best way to protect your business. Making sure your staff are aware of these common pitfalls can help you proactively fight fraud.

## Vet all invoices carefully

Scammers will often send legit-looking invoices for common office expenses in hopes they get paid without question. Educate your accounts payable personnel and keep a list of the utility companies, web hosting services and office suppliers you work with. Any bills that turn up outside of this list should be reviewed by a supervisor prior to remitting payment.

## Ensure listings and ads services are legit

Advertising your business is a great way to build a brand – so long as the directory or outlet really exists. Many entrepreneurs have been duped into giving up company info in exchange for fake listings, coaching sessions or internet ads, only to be hit with massive bills for unfulfilled services shortly after.

Should you receive calls making such claims, do your homework and be careful what you say during the exchange. Many calls are recorded and used as collateral to pressure you for payment after the fact.

## Investigate all "urgent" emails

Cybercriminals have nearly perfected their phishing emails attempts. Many pose as known vendors or internal company contacts intending to reach bookkeepers or business owners. Messages typically lead with a sense of urgency, aiming to collect payments to keep accounts in good standing or verify information about your staff.

Flag any messages that look even slightly suspicious and never click links or download information until you've verified the sender is legitimate.

## Use caution when fielding Tech Support claims

Proceed with caution any time you receive a message from an outside organization alerting you to deal with a computer security issue. They may in fact be the problem. The aim is often to enroll you for a fake service that purports to closely monitor your network, only to bill you for a maintenance program that doesn't actually exist.

Even if they're not asking for payment, the goal may still be unscrupulous. Many simply desire access to your computer files so they can extract sensitive company data or passwords.

## Manage unordered merchandise wisely

Keep a detailed list of all the office supplies and merchandise you order. Should any products show up that weren't initiated by your staff, don't get tricked into paying for them. Instruct employees to refrain from giving out the company address to any vendors offering to send free samples or mailer information, too. These interactions are often recorded and later used to "prove" you placed an order and are withholding payment.

Stopping scams from the start is a collective effort that never ends. Arming yourself and your staff with knowledge is the first line of defense when fighting fraud.