

# Aeros

A DIFFERENT WAY TO I.T.



Tax season is here, and unfortunately, cybercriminals are taking advantage of it. Recently, we've seen a rise in phishing scams targeting QuickBooks users—and we want to make sure you and your business stay protected.

## What is Phishing?

Phishing is when scammers send fake emails pretending to be from a trusted company—like QuickBooks or Intuit—to trick you into sharing personal information, clicking malicious links, or opening harmful attachments.

## How Scammers Try to Trick You:

1. Fake QuickBooks Emails or Calls: Emails that claim your account is suspended, your tax documents are ready, or payment details need updating.
2. Lookalike Websites: Links that lead to fake QuickBooks login pages designed to steal your credentials.
3. Urgent or Threatening Messages: Warnings about tax issues or account closures to create panic and push you to act fast.

## How to Stay Safe:

1. Verify the Sender: QuickBooks emails always come from @intuit.com—if you're unsure, log in directly at [QuickBooks' official website](#).
2. Think Before You Click: Hover over links to see the actual destination before clicking.
3. Enable Multi-Factor Authentication (MFA): This adds an extra layer of security to your accounts.

## If You Receive a Suspicious Email:

1. Don't click or reply.
2. Forward it to [phishing@intuit.com](mailto:phishing@intuit.com) to report the scam.
3. Reach out to us if you're unsure about an email or want to improve your business's email security.

Want to learn more about phishing protection and secure email solutions? We're here to help! Feel free to reply to this email or call us 616.997.8424.

# Aeros

A DIFFERENT WAY TO I.T.



## WINDOWS 10 END OF LIFE AND UPGRADING TO WINDOWS 11

We wanted to give you a quick heads-up so you're not caught off guard. Starting mid-April, you may notice a small popup message on your computer about upgrading to Windows 11. Don't worry, it's safe, and it's from us.

This message will only appear on computers still running Windows 10, and it's simply there to share important information about upgrading. You don't need to panic or take any immediate action—just read the message when it pops up and click OK to dismiss it. An example of what the popup will look like is below.

### Why You're Seeing This:

Windows 10 is being phased out by Microsoft, and we want to make sure your devices stay secure, supported, and up to date. This popup is just our way of giving you a friendly nudge and opening the door for any questions you might have.

### What You Can Do:

- 1.If you have questions about the upgrade...
- 2.If you'd like to check which of your workstations need Windows 11...
- 3.Or if you just want a bit of guidance...

Reach out to us! We're happy to walk you through your options for the upgrade.

Thank you for being a part of the Aeros family.

Aeros

A Different Way to I.T.

### Import Notice from Aeros IT Group

You are receiving this notification because your computer is running Windows 10, which Microsoft will stop supporting on October 14, 2025. After this date, your system will no longer receive security updates, leaving it vulnerable to threats.

To stay protected, your workstation must be upgraded or replaced with Windows 11 before the deadline.

**Act now — Scheduling will be more limited as October approaches!**

Call: (616) 997-TECH (8324)

Email: [support@aerosgroup.com](mailto:support@aerosgroup.com)

OK