BBB Tip: Your Cloud Storage Is Full… Or Is It?

Submitted by Kelvin H. Collins, President/CEO, Better Business Bureau

Serving the Fall Line Corridor, Inc. • BBB.org/central-georgia • Office: 478.742.9034 (Direct)
OFFICES: Macon: 277 M.L. King Jr. Blvd, Ste 201, Macon, GA 31201 • Augusta: 119 Davis Road, Ste 3-B, Augusta, GA 30907 Columbus: 233 12th Street, Ste 911-B, Columbus, GA 31901

Imagine receiving an email warning that your online storage is full and your family photos, important documents, and other files could soon be deleted. The message looks like it came from a company you recognize, and there's a convenient button to fix the problem. Would you click it?

Scammers are counting on that reaction. They're sending convincing emails and text messages that impersonate popular cloud storage services, hoping consumers will provide passwords, credit card numbers, or other personal information.

The BBB and FTC have specifically warned consumers about fake storage notices appearing to come from companies such as Apple, Google, and Microsoft.

The Better Business Bureau (BBB) offers these tips to help you spot warning signs and protect your information.

How the Scam Works

Cloud storage allows people to save photographs, videos, documents, and other information online rather than keeping everything on a single device. Services such as iCloud, Google Drive and Microsoft OneDrive are commonly used to back up important files.

Because many consumers rely on these services, scammers know that the possibility of losing valuable information can create immediate concern. A fraudulent message may claim that your storage has reached its limit, a payment was declined, your account has been suspended, or your files are scheduled for deletion.

The message usually includes a button labeled "Upgrade Storage," "Renew Now" or "Verify Payment."

Clicking that button may take you to a counterfeit website designed to look like the legitimate company's sign-in or payment page. Once you enter your information, the scammer may have what they need to access your account, make unauthorized charges or attempt additional fraud.

Don't Let Urgency Make the Decision

One of the biggest warning signs is pressure to act immediately. A message might claim that your photos will be permanently deleted within 24 hours or that this is your final opportunity to save your files. Scammers use deadlines and alarming language to discourage consumers from taking time to verify the warning.

Legitimate storage providers may notify customers about storage limits or billing problems. That doesn't mean every such message is fraudulent. The important distinction is how you respond. Even when a warning appears legitimate, don't use the link in an unexpected email or text to resolve the issue.

Check Your Account Yourself

The safest way to determine whether you actually need more storage is to check directly with your provider. Open the company's official app, use your device's account settings or enter the company's website address yourself. Once signed in, review your storage usage, subscription status and payment information.

If there's a genuine problem, you can address it through your account without relying on a link someone sent you. If you don't even have an account with the company sending the warning, that's another strong indication the message is fraudulent.

Look Beyond the Company Logo

Scammers can copy familiar logos, colors and layouts, making fraudulent messages appear surprisingly professional. Don't assume an email is legitimate simply because it looks like something you've received before.

Look carefully at the sender's email address. A message claiming to come from a major technology company but originating from an unrelated domain deserves suspicion. Watch for unusual website addresses, requests for passwords or verification codes, and unexpected payment demands.

Remember that a familiar company name displayed in an email does not prove who actually sent it.

What If You've Already Clicked?

If you clicked a suspicious link but didn't enter any information, close the page and avoid downloading anything it offers. If you provided your password, go directly to the legitimate company's website or app and change it immediately. Enable multi-factor authentication if you haven't already.

If you entered credit card or banking information, contact your financial institution promptly. Explain what happened and ask about protecting your account. If you downloaded software, update your security software and run a scan.

You can report suspected phishing attempts to the FTC at ReportFraud.ftc.gov and to BBB Scam Tracker at BBB.org/ScamTracker.

Protect Your Digital Memories

Whether your cloud storage contains family photographs, financial documents or years of personal files, it's worth protecting. Consider keeping a separate backup of important information so you aren't entirely dependent on one online account. Most importantly, remember that an unexpected warning is not a reason to panic.

When someone tells you your digital memories are about to disappear unless you click immediately, take a moment to verify the claim yourself. That simple precaution could prevent a storage warning from becoming a much more expensive problem.

****

Kelvin Collins is president & CEO of the Better Business Bureau serving the Fall Line Corridor, which serves 77 counties across Georgia, Alabama and South Carolina. BBB helps consumers make informed marketplace decisions, promotes trustworthy business practices and provides resources to help consumers avoid scams. To research a business, file a complaint, submit a customer review or report a scam, visit BBB.org. For assistance from your local BBB, call 800-763-4222 or email info@centralgeorgia.bbb.org.