Email threatening to reveal private data from Microsoft may be a scam

Unfortunately, criminals can easily pretend to be someone else, and that's exactly what's happening with a new fake Microsoft email that's going viral.

The saying 'when someone tells you who they are, believe them' doesn't hold true in cyberspace, where hackers run rampant. Unfortunately, it's easy for criminals to pretend to be someone else, and that's exactly what's happening with a new fake Microsoft email that's been circulating. If you've received a message from Microsoft threatening to expose your private data, it's probably a scam—even if it comes from a Microsoft account.

Why you shouldn't immediately trust a threatening email from Microsoft?

In the latest Microsoft scam, hackers exploited a vulnerability in the Microsoft 365 Admin Portal code to send emails from Microsoft.com accounts, so the messages didn't end up in recipients' spam folders.

Although they may appear to be legitimate emails, these emails claim to contain sensitive images or videos of you in sensitive situations. To prevent this content from being shared, you must pay a ransom. In other words, these emails are intended to blackmail you.

Warning : When extortion scams are paired with sexually explicit or sexually explicit media content, this is often referred to as 'sextortion.'

Warning signs to watch out for

Sadly, sextortion scams are becoming more common, prompting companies to introduce safeguards, like Instagram restricting the ability to delete photos. But for every safeguard, criminals will find a technical loophole. So we need to be able to take things seriously, in case tech companies fail.

Microsoft

Of course, the first thing to check is the username or email address. In this example, the hacker exploited a vulnerability in the Microsoft 365 Message Center's "share" option, which is often used for legitimate service

alerts. This makes the message appear to come from Microsoft.com. So the sender's address itself is not a reliable identifier.

The main red flags are the content of the message. What is the sender asking you to do? In the event of a real data breach, would a company like Microsoft demand payment in Bitcoin? The answer is no.

Don't help scammers!

Even if you realize the message is from a hacker, you may still feel compelled to pay because you want to protect your stolen media. The risk becomes more real if the sender includes personal information in the message to back up their claim.

For example, someone posted an example of one of these Microsoft emails on the Microsoft Answers forum, which included the recipient's date of birth. A date of birth is one thing—a bunch of "internet history" and secretly recorded "webcam footage" is another. Claims like this are unfounded, and it's best to report the email to Microsoft or whatever platform you received the message from.

Note : Microsoft is currently investigating this criminal activity.

If you receive an email that appears to be from a legitimate source but asks for Bitcoin, it's probably a scam. Even if hackers have figured out how to bypass spam filters, they can't hide their motives when it comes to the actual request. If your data is actually compromised in a breach, a reputable company like Microsoft or Google will have steps for you to take that don't involve cryptocurrency.

You finished reading the article "**Email threatening to reveal private data from Microsoft may be a scam**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.

© 2019 TipsMake.com