So, you use Slack eh…

I guess it's not THAT terrible they give away your passwords, right?

Yes, it's true. *Source*

In an effort (I guess) to apparently not use a unified system built by a reputable provider, many companies initially put their faith in Slack to help fill their enterprise collaboration efforts.

"Well, it's free right?"

Um, no, it's really not, there is an initial free tier, but once that trial ends you pay for members that are active in your workspace.

"So, what's the problem?"

The problem in question here is not properly maintaining a service and to thoroughly test security risks/flaws in the program.

"Bah… come on, what's the worst thing that can happen?"

The worst? Well, only time is going to tell about that, but one recent problem is…

THEY'VE BEEN LEAKING YOUR PASSWORDS

FOR OVER FIVE YEARS!

In a Slack security advisory dated August 4, 2022, users were notified that this "bug" was occurring every time users created or revoked shared invitation links.

And this "bug" (as they attempt to downplay it), took an independent security analyst to find.

They had no idea, and that's just… well, that's not good.

On top of this, Slack's response continues to be intentionally vague and confusing, in their attempt to mitigate the risk associated with this pretty remedial technical issue. When asking for feedback from frontline IT professionals, they all returned the same thought:

"Who the hell leaks password hashes?"

Who indeed.

Because this never should have been a problem, if in fact the technical team had proper processes in place like any sort of Quality Assurance (QA), which apparently, they do not. We'll get to what this means soon, but it's also not good.

This is the company you chose to trust with your data and legal/medical/financial communication?

So, what exactly happened?

In full disclosure and fairness here, it's not like Slack directly or even purposely sent passwords directly to someone. What happened was Slack was sending passwords that were included in the network packets which commonly include data that's normally used or seen by the recipient.

An example of this data packet inclusion are HTTP headers, which are meant to be instructions to your browser, not data for display in the web page you're looking at. So, while it is being passed, it's not actually something you would commonly see or even know to look for.

Unless you're a hacker… Then it's exactly what you're looking for.

This data in question is that's seemingly irrelevant or invisible to users ends up in logs, especially in firewall logs, where it could be preserved indefinitely, just waiting for someone to come along and, well, snatch it up.

That's the really bad news, mainly because if this is a problem, it greatly calls into question what other vulnerabilities are there? And have they also existed for several years? What are the other issues they don't know exist yet and do they even have QA processes? Surely, they must, but if it wasn't caught for 5 years, what more needs to be disclosed and are they hiding it?

I don't know, mainly because we focus on Best-in-class, Unified Solutions from Microsoft because by unifying communications through a single pane of glass interface, we eliminate a variety of risks, concerns, and compatibility issues. This is because EVERYTHING is delivered by the same company, through a very familiar interface that even possibly includes your operating system and web browser, resulting in one centralized place for all communication, collaboration, administrative and conferencing needs.

In The Cloud Technologies are experts at providing Unified Communications as a Service, potentially even bundled with a variety of managed services, all delivered at a fixed monthly price per user. This includes IT Support, Cyber Security and Backup/Disaster Recovery, as well as Professional Services and Augmented Staffing.

We do greatly value quality assurance, because we stay with our clients every step of the way and don't just collect our payment and become hard to find. Through our all-inclusive approach, everything is commonly included, so if something arises, we fix it, and we don't bill the client.

For a more detailed analysis on the benefits of a unified communications system, see our recent blog article on our website, "*If You're Not Using Microsoft Teams, Then You're **NOT** Collaborating*."

If you are currently using Slack, we recommend switching to Microsoft Teams. However, if your not ready to transition to a new system, then we recommend turning on 2FA if you can. 2FA, or two-factor authentication, means that you need not only your password to login, but also a one-time code that changes every time. These codes are typically sent to (or generated by) your mobile phone and are valid only for a few minutes each. This means that even if someone does crack your password, it's not enough on its own for them to take over your account.

For more technical information on this problem, check out this article, which explains how it happened and a ton of very technical information on passwords being hashed, salted, and stretched, which are at the heart of the issue. https://nakedsecurity-sophos-com.cdn.ampproject.org/c/s/nakedsecurity.sophos.com/2022/08/08/slack-admits-to-leaking-hashed-passwords-for-three-months/amp/

If you need more help on these issues or anything else, we are only a phone call away and would genuinely love to speak with you. Call In The Cloud Technologies today, 888-603-1033.

We at would love to show you a demo and explain the many benefits that come with a Unified approach to Communications and Collaboration, by Microsoft. Feel free to call us at 888-603-1033.