3

SIMPLE STEPS

TO IMPROVE SECURITY

IN YOUR SLACK WORKSPACE

Beamed to your screen

By your friends at 🦜 **Polly**

We work in Slack.

If you're reading this,
you probably do, too.

We care about security.

If you're reading this, **you probably do, too**.

So we put together a list of simple, yet effective things you can do in order to **improve security in your Slack workspace in just a few minutes**.

It's up to you and your colleagues to be **good stewards** of the data you're entrusted with.

Luckily, it's easier than you might think to make **meaningful improvements** to the security of your Slack workspace.

This is not
a comprehensive manual.

There is no substitute for **due diligence**, **expertise**, or **professional security advice**.

But this *is*
a great starting point.

So let's do that.

Let's get started.

Did you know...

Research based on over 30 million users worldwide, across over 600 enterprises found that **21% of files** in the cloud **contain sensitive data**?*

Or that...

80.3% of the organizations in the study experienced at least one compromised account threat **per month?**
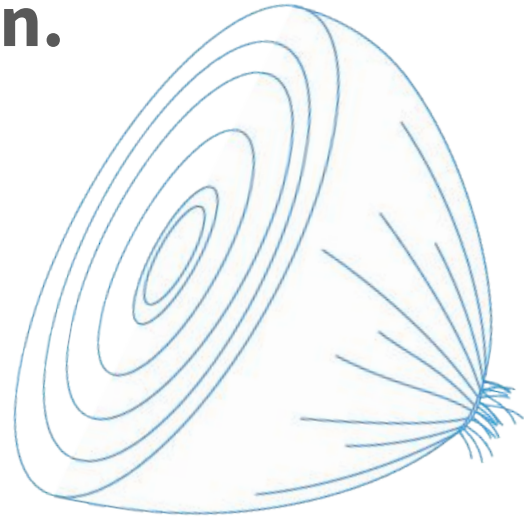
Good Security

Helps insulate you and your team from similar security events. **But what does good security look like <u>in practice</u>?**

Good security looks like an **onion**, wrapped around a chunk of gold.

If you peel back one layer to get at the gold, all you get is **more onion**.
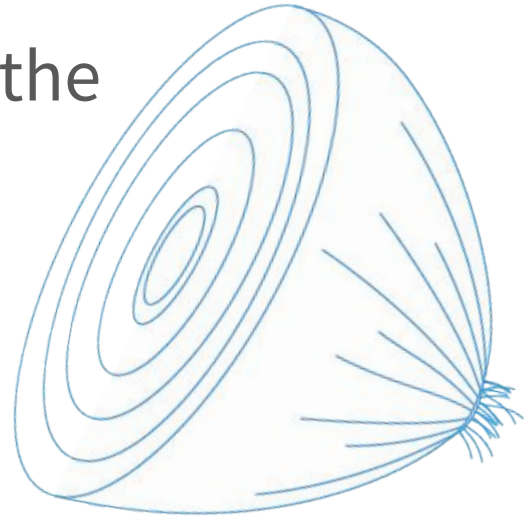
So let's add some layers

to your Slack security onion.

Security Tip
Number One:

Manage and Control Access

Managing and controlling access means ensuring everyone has all the data and resources they need at any given time, and none that they don't.

You can manage access manually, or with an automated system. Either way, the key is to have a process in place that is **followed consistently**.

Learn more

Security Tip
Number Two:

Require Two-Factor
Authentication (2FA)

Two-factor Authentication (2FA) adds another simple, yet powerful **layer of security** to your workspace.

With 2FA required, users need to enter a **time-sensitive single-use code** that only they can access, in order to authenticate a new device.

This means that **with 2FA required**, usernames and passwords alone are not enough for an attacker to gain access to your Slack Workspace.

Learn more

Security Tip
Number Three:

Stick to apps available
In Slack's App Directory

While there's no way to know with **100% certainty** that an app is safe, Slack vetts every app in its directory.

Some apps list detailed security and compliance information right in their directory listing to help you evaluate.

As an administrator, you can limit app installations your workspace to apps from the **Slack App Directory**.

You can also control which types of apps are available to your team.

Learn how

That's it! Taking these three steps can make a meaningful improvement to your Slack workspace security.
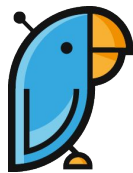
Was it easier than you expected? We hope so.

So, are you ready to take it to the next level?

There are still **many improvements** you can make to your Slack workspace security -- several of which we cover in

"A Busy Admin's Guide to Slack Security."

Let's go!

Polly

Polly is a tool used by teams worldwide to securely and contextually gather **continuous insights** into their most important **people-driven processes**.

See how it works!