# Study shows which messengers leak your data, drain your battery, and more



## reader comments

92 with 64 posters participating

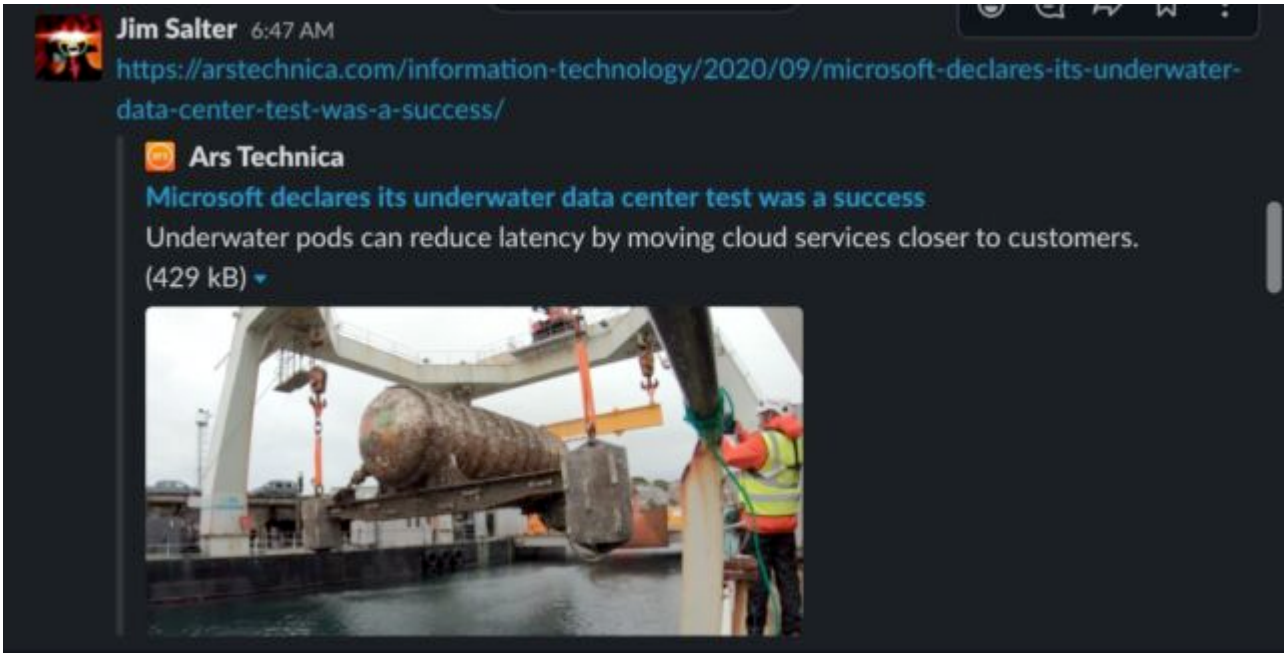
## Share this story

Link previews are a ubiquitous feature found in just about every chat and messaging app, and with good reason. They make online conversations easier by providing images and text associated with the file that’s being linked.

Unfortunately, they can also leak our sensitive data, consume our limited bandwidth, drain our batteries, and, in one case, expose links in chats that are supposed to be end-to-end

encrypted. Among the worst offenders, according to research published on Monday, were messengers from Facebook, Instagram, LinkedIn, and Line. More about that shortly. First a brief discussion of previews.

When a sender includes a link in a message, the app will display the conversation along with text (usually a headline) and images that accompany the link. It usually looks something like this:




For this to happen, the app itself—or a proxy designated by the app—has to visit the link, open the file there, and survey what's in it. This can open users to attacks. The most severe are those that can download malware. Other forms of malice might be forcing an app to download files so big they cause the app to crash, drain batteries, or consume limited amounts of bandwidth. And in the event the link leads to private materials—say, a tax return posted to a private OneDrive or DropBox account—the app server has an opportunity to view and store it indefinitely.

The researchers behind Monday's report, Talal Haj Bakry and Tommy Mysk, found that Facebook Messenger and Instagram were the worst offenders. As the chart below shows, both apps download and copy a linked file in its entirety—even if it's

gigabytes in size. Again, this may be a concern if the file is something the users want to keep private.

[embedded content]
Link Previews: Instagram servers download any link sent in Direct Messages even if it’s 2.6GB
It’s also problematic because the apps can consume vast amounts of bandwidth and battery reserves. Both apps also run any JavaScript contained in the link. That’s a problem because users have no way of vetting the security of JavaScript and can’t expect messengers to have the same exploit protections modern browsers have.

[embedded content]
Link Previews: How hackers can run any JavaScript code on Instagram servers.
Haj Bakry and Mysk reported their findings to Facebook, and the company said that both apps work as intended. LinkedIn performed only slightly better. Its only difference was that, rather than copying files of any size, it copied only the first 50 megabytes.

Meanwhile, when the Line app opens an encrypted message and finds a link, it appears to send the link to the Line server to generate a preview. “We believe that this defeats the purpose of end-to-end encryption, since LINE servers know all about the links that are being sent through the app, and who’s sharing which links to whom,” Haj Bakry and Mysk wrote.

Discord, Google Hangouts, Slack, Twitter, and Zoom also copy files, but they cap the amount of data at anywhere from 15MB to 50MB. The chart below provides a comparison of each app in the study.

| | End-to-End Encrypted | Unauthorized Copies of Private Information | Getting Servers to Download Large Amounts of Data | Crashing Apps and Draining the Battery | IP Exposure | Leaking Encrypted Links | Running Potentially Malicious Code on Link Preview Servers |
|---|---|---|---|---|---|---|---|
| **Discord** | No | Up to 15 MB | No | No | No | No | No |
| **Facebook Messenger** | No | Unlimited! | **Yes** | No | No | No | **Yes** |
| **Google Hangouts** | No | Up to 20 MB | No | No | No | No | No |
| **iMessage** | Yes | No copies | No | No | No | No | No |
| **Instagram** | No | Unlimited! | **Yes** | No | No | No | **Yes** |
| **LINE** | Yes | Up to 20 MB | No | No | **Yes (Fixed!)** | **Yes** | No |
| **LinkedIn** | No | Up to 50 MB | **Yes (Through JavaScript)** | No | No | No | **Yes** |
| **Reddit** | No | No copies | No | **Yes (Fixed!)** | **Yes (Fixed!)** | No | No |
| **Signal** | Yes | No copies | No | No | No | No | No |
| **Slack** | No | Up to 50 MB | No | No | No | No | No |
| **Threema** | Yes | No copies | No | No | No | No | No |
| **TikTok** | No | No copies | No | No | No | No | No |
| **Twitter** | No | Up to 25 MB | No | No | No | No | No |
| **Viber** | Yes | No copies | No | **Yes** | No | No | No |
| **WeChat** | No | No copies | No | No | No | No | No |
| **WhatsApp** | Yes | No copies | No | No | No | No | No |
| **Zoom** | No | Up to 30 MB | No | No | No | No | No |

Talal Haj Bakry and Tommy Mysk

All in all, the study is good news because it shows that most messaging apps are doing things right. For instance, Signal, Threema, TikTok, and WeChat all give the users the option of receiving no link preview. For truly sensitive messages and users who want as much privacy as possible, this is the best setting. Even when previews are provided, these apps are using relatively safe means to render them.

Still, Monday’s post is a good reminder that private messages aren’t always, well, private.

“Whenever you’re building a new feature, always keep in mind what sort of privacy and security implications it may have, especially if this feature is going to be used by thousands or even millions of people around the world,” the researchers wrote. “Link previews are a nice feature that users generally benefit from, but here we’ve showcased the wide range of problems this feature can have when privacy and security concerns aren’t carefully considered.”

https://arstechnica.com/?p=1717263