UNSANCTIONED CHAT

The Use of Group Chat Tools at Work

SPIDEROAK

Group chat tools are taking center stage in everyday business.

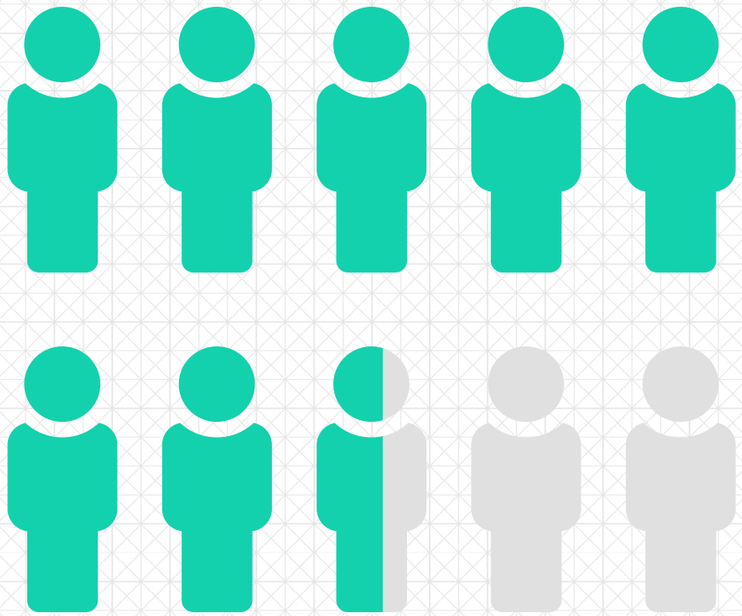
INTRODUCTION

Employees are using group chat to help them streamline projects, share files, minimize their email inbox, and bolster company culture. Features like integrated video conferencing, GIFs, and emojis are also fun and easy to use. Enterprises are following their employees' lead and adopting officially sanctioned group chat tools to foster team collaboration.

However, on closer inspection, employees are using more than their approved chat tools to communicate with others. And on these unsanctioned apps, employees admit to sharing sensitive company information (like passwords or financials) and customer data. This means employees could be leaking important company information that puts the business at risk without their employer's knowledge.

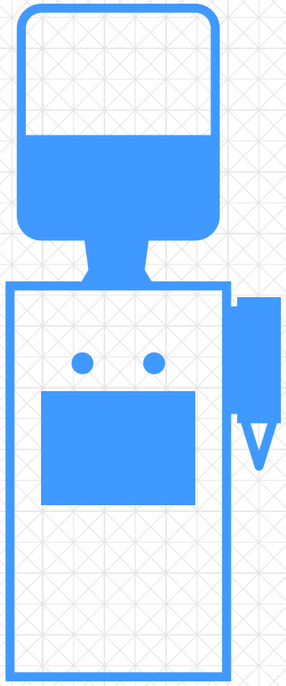
This survey examines the way employees in varying industries communicate online, what kinds of information they share on unsanctioned group chat tools, and why they choose to use tools that aren't authorized by their employers.

Overall, the survey found that employees who use authorized group chat tools also use unsanctioned tools to communicate with one another. Three-quarters of respondents reported that they share sensitive company information on unsanctioned tools, such as planning, financial, or customer information. With the consistent rise of data breaches and cyberattacks, employers must be vigilant to the risks that unsanctioned and unsecure tools pose to a company. Companies who turn a blind eye could find themselves with a much bigger problem than employees' use of rogue group chat tools.



76.8% of respondents who use authorized group chat tools reported that they also use unsanctioned group chat tools to communicate.

Despite companies implementing an authorized group chat tool, many employees are using unsanctioned tools.



47.8%

use group chat tools to communicate with coworkers

WHO IS CHATTING

Nearly half of survey respondents reported that they use group chat tools to communicate with coworkers (47.8 percent). Of this percentage, the majority of respondents always, often, or sometimes (18.8 percent, 22.2 percent, and 35.8 percent, respectively) use unsanctioned tools to communicate with team members. Of the population that uses unsanctioned group chat tools despite having an officially sanctioned tool at work, nearly one quarter works in IT, and almost 15 percent work in leadership (24.4 percent and 14.9 percent, respectively).

Search Channels

COMPANY

#Who is Chatting

#Why Chat

#Chats About

Employees use unsanctioned group chat tools because they are easier and/or more fun to use than the authorized group chat tool their employer provides.

WHY CHAT

Skype, iMessage, WhatsApp, Slack, Facebook Workplace, office intranet messaging systems, Microsoft Teams, HipChat, Semaphor, and others are among the group chat tools that respondents reported using to communicate in the workplace. Respondents indicated that they use unsanctioned tools because they are easier or “more fun” to use (55.7 percent and 27.5 percent, respectively) than the group chat tools their company implements.

Search Channels

#Who is Chatting

#Why Chat

#Chats About

Easier to Use (55.7%)

More Fun to Use (27.5%)

N/A (27.1%)

Don’t Want Their Manager or Bosses Spying on Their Conversation (13.2%)

Don’t Want to Learn a New Tool (3.1%)

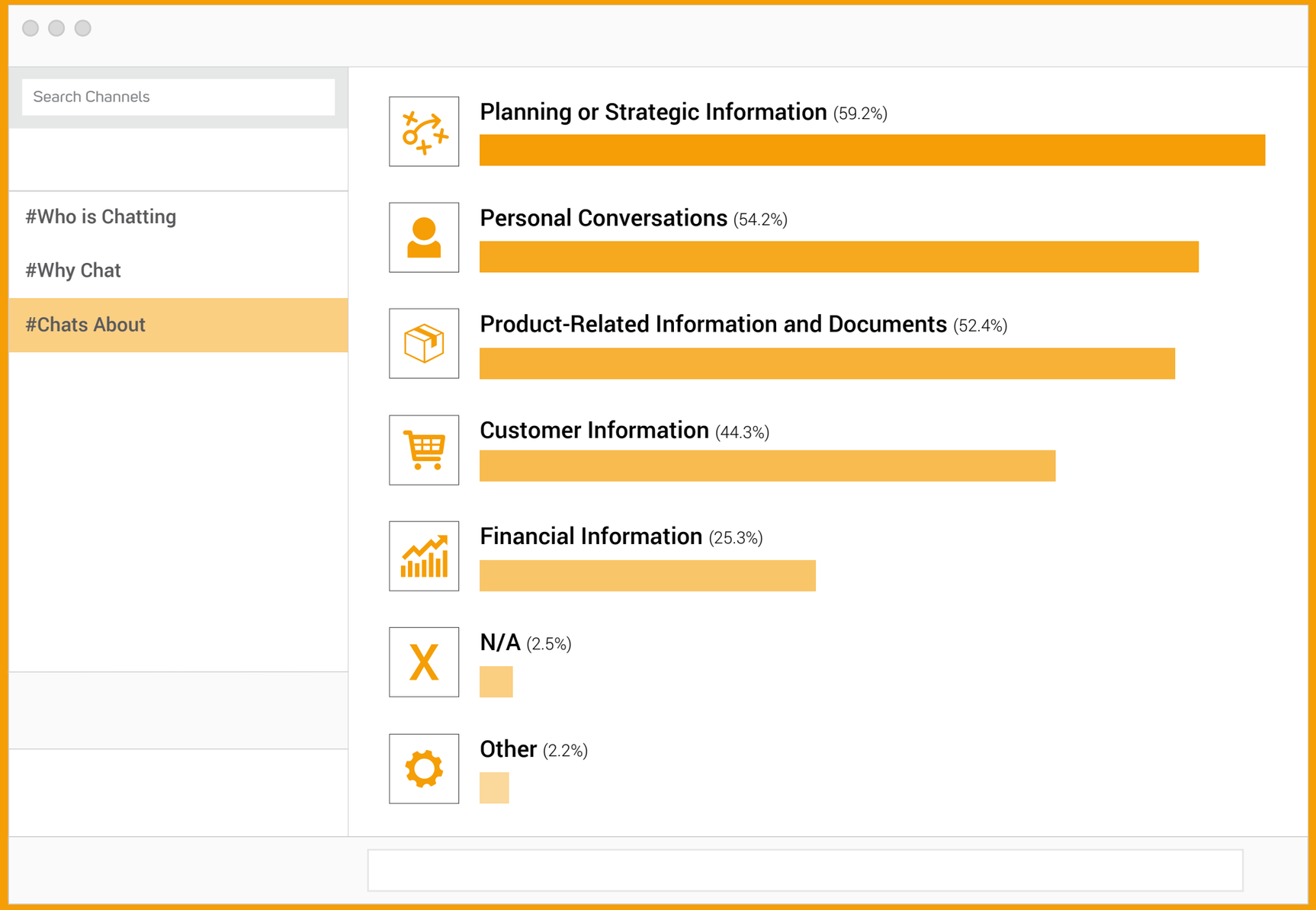
Employees who share sensitive information on unsanctioned group chat tools lack personal experience in security breaches or identity theft.

76.4%

to their knowledge, have not had their identity stolen or had an online account compromised

CHATS ABOUT

The majority of respondents who have an authorized group chat tool, but use unsanctioned tools, reported that they share sensitive company information on these tools, such as planning or strategic information, product-related information and documents, customer information, and financial information (59.2 percent, 52.4 percent, 43.4 percent, and 25.3 percent, respectively). Most of these respondents (76.4 percent) reported that they have not, to their knowledge, had their identity stolen or had an online account compromised. They also didn't know of any friends, or coworkers, who have had their identity stolen or an online account compromised. At the same time, this group of respondents also indicated that their company had always, often, or sometimes stopped using or chose not to use a product because of a poor security record (14 percent, 12.2 percent, 40.2 percent, respectively).


Search Channels
#Who is Chatting
#Why Chat
#Chats About
Planning or Strategic Information (59.2%)
Personal Conversations (54.2%)
Product-Related Information and Documents (52.4%)
Customer Information (44.3%)
Financial Information (25.3%)
N/A (2.5%)
Other (2.2%)

When it comes to securing an organization, leadership and IT must start an open dialogue around the importance of using sanctioned group chat tools.

CONCLUSION

The results of this survey indicate that employees use unsanctioned group chat tools because the tools are easier and/or more fun to use, and they haven't experienced firsthand the damage that identity theft or an account compromise can cause. With those working in leadership and IT comprising the largest portion of offenders, employees may not feel compelled to follow the rules when those implementing them are also using unsanctioned tools. When it comes to securing an organization, leadership and IT must start an open dialogue around the importance of using sanctioned group chat tools. This indicates that while they are aware that a security concern exists, they are not motivated or hindered by security concerns. Leadership and IT must start an open dialogue around the importance of using sanctioned group chat tools from a security standpoint. In doing so, companies will be at less risk for data breaches that result in the violation of sensitive customer information.

METHODOLOGIES

SpiderOak sponsored an independent survey of 600 full-time workers ages 21 and older who live in the United States. Of the respondents, a majority were between the ages of 25 and 34 (35.3%) and 35-44 (30.2%), with seasoned professionals aged 45 to 64 making up 18.2% of the responses. Annual household incomes ranged from $25,000 to more than $500,000, with 28% of respondents reporting $50,000 – $70,000, 25% reporting $25,000 – $50,000 in annual income, and 22% of respondents reporting $100,000 to more than $500,000 in annual income. Company sizes ranged from 50 employees or fewer to 500 employees or more, with 39.1% of respondents reporting they work for a company with 50 employees or fewer, 33.6% reporting they work for a company with 500 employees or more, and 27.1% reporting they work for a company with 51-500 employees.

40.2%

aware that their company has stopped using or chosen to not use a product because of a poor security record

ABOUT SPIDEROAK

SpiderOak gives you control of your data online. The company's secure cloud backup solution, SpiderOakONE, and group chat and file sharing tool, Semaphor, are designed to be 100% Zero Knowledge, innovative, reliable, and affordable. For over ten years, SpiderOak has been helping individuals, groups and enterprises protect their most important information with end-to-end encryption. Feel safe again.

spideroak.com