Remote Work Online Behavior Report

ManageEngine

The COVID Behavior Report

Due to COVID-19, more people are working from home than ever before. Many of these users conduct work from corporate and personal devices, which can potentially compromise sensitive corporate data. As more users work from home, we're seeing a concerning paradigm: an acceleration of risky online behavior combined with increased user confidence in online tools.

ManageEngine surveyed nearly 1,500 employees between March and June 2020 as much of the world worked from home. We inquired about users' web browsing habits, opinions about AI-based recommendations, and experiences with chatbot-based customer service. Through the survey, we were able to assess the current online landscape, as well as the ramifications for IT professionals. Here's what we found.

Dangerous online activity and a lack of user self-regulation highlights the need for security tools and user behavior analytics.

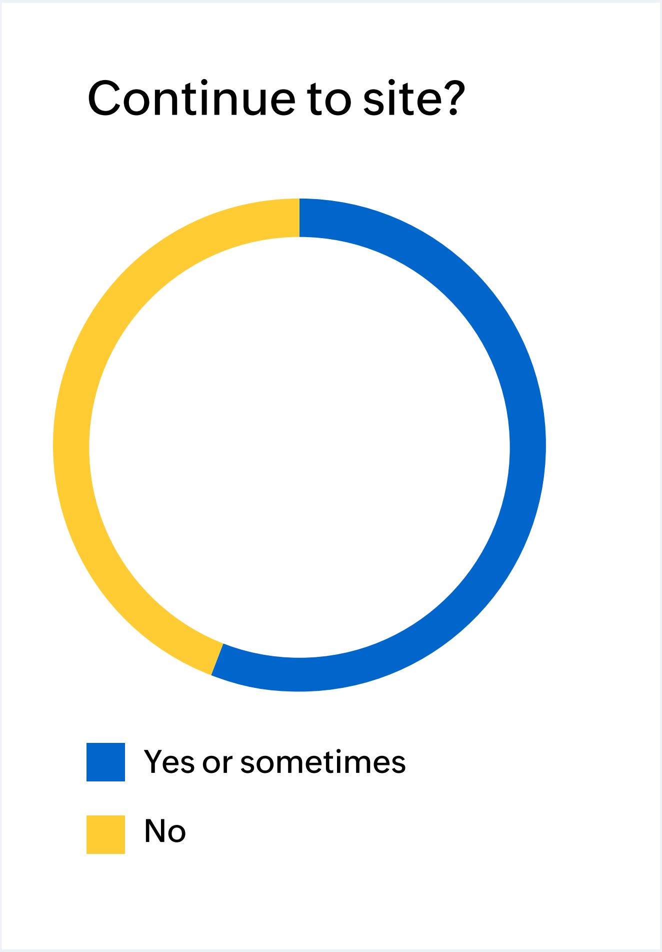
From the results of these two surveys, some clear issues emerge. Firstly, users—especially younger users—are increasingly acting dangerously online. By visiting websites that have been compromised and returning to sites where their information was stolen, users have shown that they are not self-regulating. Secondly, this precarious situation is exacerbated as many enterprises do not enforce restrictions on corporate devices. Without the enforcement of adequate restrictions, there is a greater likelihood that users will make sensitive corporate information available to bad actors.

To complicate the matter further, shadow IT is on the rise as many employees use personal devices to access corporate data. Enterprise assets should be accessed via VPN whenever possible, and IT professionals should continuously track user behavior. With proper security tools and user behavior analysis tools, enterprises can be aware of any anomalous and potentially dangerous activity undertaken by any of their users.

With the right security tools, enterprises can gauge the safety levels of websites—even before an employee visits a site. Just by looking at the URL, one can assess whether it is an algorithm-generated URL or an actual URL. The number of vowels, sequential consonants, and total number of alphanumeric characters can reveal a great deal about a potentially harmful website.

Additionally, seeing as the majority of survey respondents failed to self-regulate their potentially dangerous internet activity, user behavior analytics are more important than ever. By employing such analytics, it is easy to identify unusual activity. Enterprise IT management teams can identify users’ past usage patterns, and then flag any activity that deviates from the users’ normal baseline behavior.

Risky online behavior



After receiving a warning that a website was insecure, 54% said they would still visit the site.

An alarming number of respondents (29%) said “yes,” they would continue visiting a website after receiving a warning from their web browser that the site was insecure. Another 25% said they “sometimes” would continue onto the site.

Respondents who said “yes” or “sometimes” typically skewed younger. A sizable number (42%) of 18-24 year olds said they’d sometimes continue onto the site; remarkably 40% of 25-34 year olds and 50% of 35-44 year olds said they would continue.

As users—especially younger users—engage in increasingly risky behavior online, security tools and user behavior analyses are more important than ever.

Risky online behavior

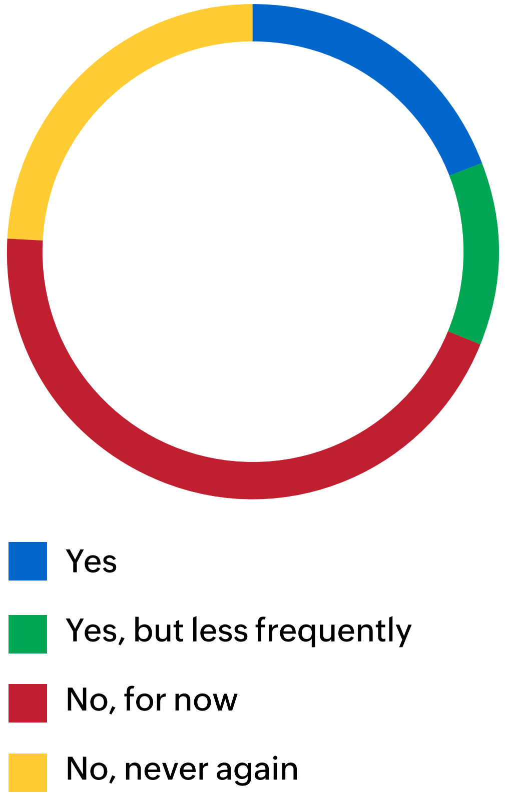
Only 19% said they'd never return to a website where their information was stolen.

When asked whether they would revisit their favorite website after a hack in which their information was stolen, over a third (36%) of respondents said "yes" or "yes, but less frequently." Remarkably, only 19% vowed never to return to the compromised website.

Of those who unequivocally answered "yes," 43% were in the 35-44 age range. Moreover, older respondents were far more likely to say they would never return to the site after their information was stolen.

Nearly half (48%) of those who said they'd never return to the compromised site were aged 55 and over.

Would you visit the website again



Remote work issues

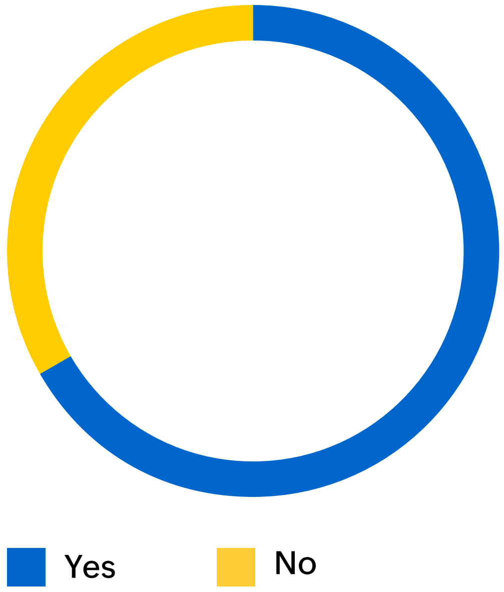
Of those respondents who were provided corporate devices, 37% said there were no restrictions on these corporate devices.

The majority of respondents (63%) said they had been provided with a corporate device, and 72% said these tools were remote work friendly.

That said, a significant portion (37%) of respondents reported that their organizations do not enforce any restrictions on the corporate devices.

Without restrictions, it is likely that some users are accessing insecure websites and exposing sensitive enterprise data.

Does your organization enforce any restrictions on your corporate devices?

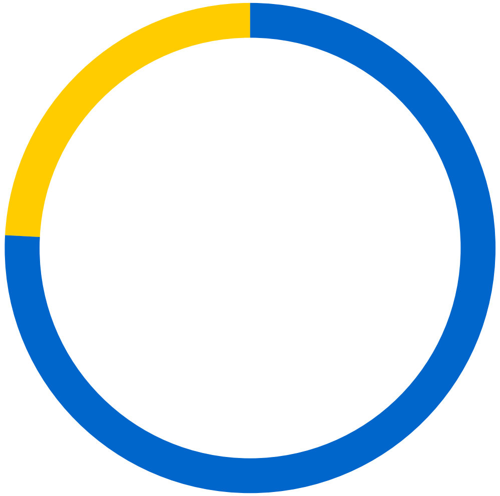


Users are increasingly comfortable with AI-based customer support and recommendations, which in turn can create a bevy of opportunities for IT teams and service desk personnel.

As users become more comfortable engaging with AI-enabled support, service desks can continue to use AI to answer frequently asked questions and automate everyday tasks. AI-based chat support can answer questions that occur on a relatively frequent basis, such as a user's inability to access a remote printer or server, or logging a complaint that a VPN or internet is down. Of course, AI can also identify and automate the solution to the users' problem as well.

It bodes well that consumers are satisfied with chatbot-based support, as IT teams can continue to use chatbots for users' information retrieval purposes, which in turn will free up time for service desk personnel to focus on other, more important tasks.

Artificial intelligence: chatbot-based support



🟦 Excellent or Satisfactory experience

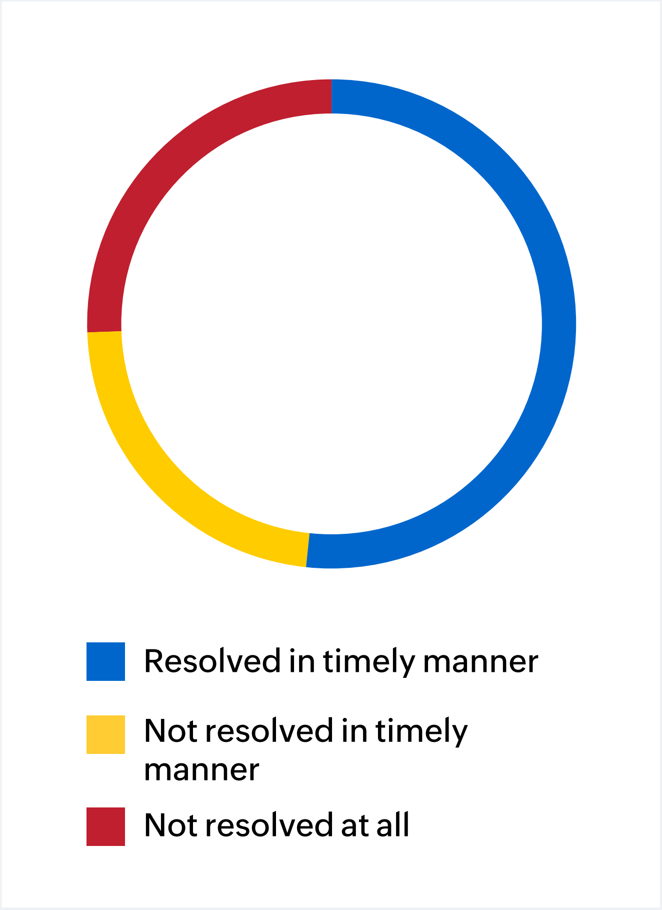
🟨 Disappointing experience

76% said their experience with chatbot-based support was "excellent" or "satisfactory."

When asked to assess their experiences with chatbot-based customer support, respondents were overwhelmingly positive. Roughly three out of every four (76%) users described their chatbot-based customer support experience as either "excellent" or "satisfactory."

The fact that only 24% of users reporting being "disappointed" with chatbot-based customer support shows how far AI-based chat support has come in recent years.

Artificial intelligence: chatbot-based support



The majority (55%) of users said their issue was resolved in a timely manner.

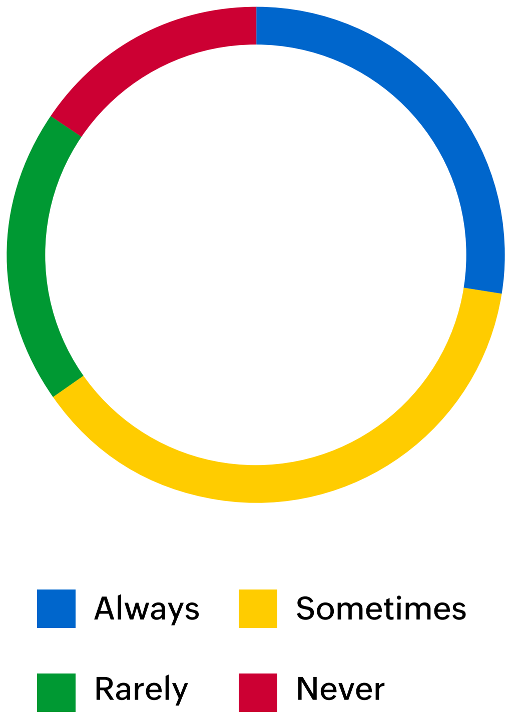
As a caveat, respondents were a bit divided over generational lines. Older users were far less likely to have a positive experience with chatbot-based support.

While only 27% of all respondents said their issue was not resolved, nearly half (48%) of respondents aged 65+ said their issue was not resolved.

Generally speaking, users—especially younger users—seem increasingly comfortable engaging with chatbot-based support.

Artificial intelligence: recommendations

Would you trust AI to make accurate recommendations?



The majority of people (66%) said they would trust AI's recommendations.

Respondents were overwhelmingly amenable to recommendations from AI. Asked if they would trust AI to make accurate recommendations during online shopping, 27% said "always"; 39% said "sometimes," and only 15% said "never."

Older generations were warier of AI-based recommendations; in fact, 25% of 55-64 year olds and 32% of those aged 65+ said they'd "never" trust such recommendations.

On the consumer front, users now tend to trust AI recommendations, which suggest there is an increased confidence in AI-based recommendations, more generally.

The Impact on IT: Increased Regulation and AI Adoption

Seeing as the majority of those working from home have shown a reluctance to self-regulate their online behavior, it is important that businesses place restrictions on corporate devices and actively gauge the safety level of websites. Additionally, whenever possible, enterprise assets should be accessed via VPN, and user behavior analysis tools should be used to identify any anomalous behavior.

With so many people embracing chatbot-based support, we also recommend embracing AI tools. Younger users are particularly comfortable engaging with artificial intelligence, so at the very least it makes sense to use such tools to answer the service desk's FAQs and to automate the solutions to users' most frequent problems. Doing so will save you valuable time and money down the road.

Hopefully, we will soon see a post-COVID world in which we're not all working from home; however, until then, IT personnel with the right security tools and user behavior analysis solutions can help keep corporate data safe. Now more than ever, the safety of your company data rests in the hands of your IT personnel.

About ManageEngine

ManageEngine crafts the industry's broadest suite of IT management software. We have everything you need — more than 90 products and free tools — to manage all of your IT operations, from networks and servers to applications, service desk, Active Directory, security, desktops, and mobile devices.

Since 2001, IT teams like yours have turned to us for affordable, feature-rich software that's easy to use. You can find our on-premises and cloud solutions powering the IT of over 180,000 companies around the world, including nine of every ten Fortune 100 companies.

As you prepare for the IT management challenges ahead, we'll lead the way with new solutions, contextual integrations, and other advances that can only come from a company singularly dedicated to its customers. And as a division of Zoho Corporation, we'll continue pushing for the tight business-IT alignment you'll need to seize opportunities in the future.

8 out of 10
biggest healthcare companies

9 of every 10
Fortune 100 companies

8 out of 10
largest financial services companies

trust ManageEngine to run their IT.

ManageEngine

www.manageengine.com

ManageEngine/ ManageEngine/ ManageEngine/