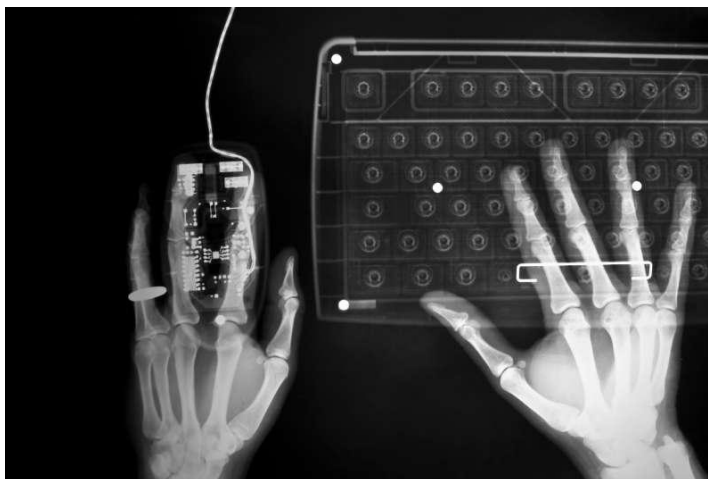


Yes, Your Employer Knows Exactly What You're Doing Online

M money.com/employer-browsing-data/

Many companies featured on Money advertise with us. Opinions are our own, but compensation and in-depth research determine where and how companies may appear. Learn more about how we make money.



Sebastian Alberto Greco—Getty Images

Chances are, if you have an office job, you've used your work computer for activities that don't necessarily relate to your day-to-day tasks.

So how paranoid should you be about being monitored?

If you're using a company computer (or wifi connection), your employer can not only monitor your work email and projects, but they can log your key strokes, including on "private" sites like Facebook or your personal email account. This is also true of company-provided cell phones (employers can even track your whereabouts given your phone's GPS).

"If you use your email on a company-owned device or even the office wifi network, you should have no expectation of privacy," says Paul Bischoff, privacy advocate at Comparitech.com. "Many companies that actively monitor employee email ask new hires to sign a waiver confirming that the company can access your email, but even those that don't offer such a waiver can still do so." (The legality of this varies state-by-state.)

"The only case in which an employee might have a reasonable expectation of privacy," writes L.V. Anderson in Slate, "would be if the employer explicitly stated that employees should have such an expectation." But that's few and far between.

Most employees have a unique login that gives them restricted access to work computers and networks. Amna Rizvi, the editor of GadgTecs.com, says that companies typically keep a log of activities for every unique user, which they can then monitor if they choose to.

A typical log might look like,

```
[time stamp] open Solitaire
[time stamp] close Solitaire
[time Stamp] Open Firefox
[...] open website ....
```

And on and on, says Rizvi. So there really is no hiding the sites you're visiting (or how long you spend on them).

But just because they *can* monitor you doesn't mean they *will*.

"We can do this but we haven't done it yet," Rizvi says. "I suspect large companies do keep a record, but might not look at the logs unless a legal issue comes up."

And in fact, most of the monitoring/information interception done on your company network is done for security purposes. All it takes is one click to transfer certain viruses or open up a company's network to hackers, which means firms need to be vigilant about what their employees are doing online.

"There could be some Intellectual Property issues and other confidential information that the company wants to control," says Michael Edelberg, co-founder of Viable Operations/Bespoke Digital Solutions, a cybersecurity firm. "Rogue cloud accounts and emails are a vector for hackers as is your social media...you might be opening a threat vector that wants access into your company."

However, they may also monitor someone if he or she is a low performer or there are reasons to suspect the employee is using office time inappropriately, says Michael V.N. Hall, a technology consultant, who has reviewed employee tech habits in the past. Hall says IT departments review things like how much network an employee is using compared to others, large deposits of pictures or videos, web content filters for disallowed categories (such as social media

or pornography), and the log in and log out times for those already on a concern list.

"In one situation, our company had an employee email a large volume of pictures from her recent vacation to her boyfriend," says Hall. "The size of these pictures bottle-necked our business email platform for several hours, slowing down critical business emails."

If you're worried about what your employer can monitor, Edelberg suggests actually reading the manual you likely received on your first day on the job. And it's probably best to send vacation photos to your boyfriend after hours.