live mint

Tue, Sep 06 2016. 09 05 PM IST

What not to do on your office PC

Whether it’s buying groceries online or downloading porn, your company can track your data

Resist the temptation to browse shopping websites on your company’s device. Photo: iStock.

An email to the boss while liking food photos on Facebook? Working on a presentation while paying electricity bills and ordering evening meals online? Most of us, at one point or another, have done personal things on our office computer. But we tend to forget that the company can monitor everything we do on our official device, be it a laptop, a smartphone or a tablet.

“You should not expect privacy while using company-given devices, irrespective of whether it is during or outside working hours,” says Vikram Shroff, head of HR (human resource) Law at Nishith Desai Associates, a corporate law firm based in Mumbai.

Legally, every company has the right to access employees’ office laptops and smartphones.

What can my company track?

It’s a no-brainer that your official email and your Web browser activities are tracked, says Nitin Chandrachoodan, associate professor at the Indian Institute of Technology, Madras. “Every communication your device does with the Internet, including office emails and sites visited on a browser, goes through the company’s servers and they routinely keep a copy of it,” he says. Though it’s a rampant abuse of privacy, your organization’s information technology (IT) team can also employ processes that let them track personal emails, phone calls, messages or social media posts.

“Through an SSL (secure sockets layer) interception, usually used to filter out viruses, an administrator can intercept your log-in and read what’s being sent back and forth between your account and the Internet, even on HTTPS secure sites,” says Chandrachoodan.

It’s the same with smartphones and tablets. All the IT team needs to do is install a monitoring app to find out what you’re doing with that smartphone. “This app can re-route all information through the company server, giving details of which apps you use, for how many hours and at what times,” he adds. The purpose, however, is not to spy on you, but to protect the company legally and to protect its copyright work, adds Chandrachoodan.

When could I get into trouble?

Every company has a list of red flags on their employee’s usage of the Internet. These include inappropriate websites, job sites, e-commerce websites and social media sites, which will put you on the IT team’s radar, says Garvita Chaturvedi, HR strategy, inclusion and business partner at Unilever, a consumer products multinational. Misuse of your official device can call for a verbal counselling session or a written complaint; it could even deprive you of a promotion. In extreme circumstances, you might get fired or the company might file a legal suit against you. “The thumb rule is: Would you be safe if what you’re doing on your laptop is seen by your team members or your boss? If you’re not, don’t do it,” adds Chaturvedi.

We list a few things that you should definitely not try on a company-given device.

Porn’s the obvious one

Just because you’re opening the website in the Incognito mode of your browser (Chrome, Firefox, etc.), or it’s really late in the night, or you’re in another country, don’t think you’ll get away with browsing porn on company devices, even if you open the site for a few minutes. “Any inappropriate website, especially porn sites, will get you fired,” says Chaturvedi. Sometimes, you might have to face legal action too.

Don’t connect a USB

Never connect an external hard drive or a USB to the office PC that is connected to the company’s network, even if it is to only transfer your

favourite music on to the device or to transfer files to take back home. Anything that can bring or transfer data from outside the network, such as USBs, CDs and Bluetooth, is a threat to the company—it could bring in a deadly virus, leak sensitive data to outsiders or transfer illegal data to the machine, making the company vulnerable to a lawsuit, says Chandrachoodan. “Usually, the company admin would have a software in your laptop that would alert them when a USB drive is plugged in. If you do, they would typically want to know what you did with it,” he adds.

Abstain from shopping

You get an email that tells you about your favourite brand’s collection being available on discount. Sounds tempting, but it’s best not to give in. “E-commerce websites are red flags in most companies,” says Chaturvedi. A little bit of browsing may be ignored, but you don’t want to be an employee who is always on Flipkart or Amazon. The tag doesn’t sound great, especially when it’s time for the next appraisal cycle.

Don’t browse medical websites

Wondering what that pimple on your buttock is all about? Resist the urge to search for an answer on your office laptop. Your employers may not mind, but remember that whatever you look at and whatever sites you visit, the communication may not be private. “Refrain from using devices owned by the company for any personal, confidential or sensitive matter,” says Shroff.

Avoid torrent or streaming

It might be a legal software or a rare e-book that you’re downloading, but this could get you into trouble. The problem is that a majority of torrent websites are used to distribute illegal copyrighted software, something a company can’t allow on its devices and network, says Chandrachoodan. “Ten minutes of torrent might be ignored, but the moment you do a download that takes hours, the IT team is likely to send a report to your manager,” he says. The same goes for streaming movies or videos excessively unless they’re part of the job. It might be ignored once or twice, but if it comes with poor performance, expect a call from HR.

Don’t look for another job

Long hours of browsing through job websites will certainly not give your employer a good impression of you, says Chaturvedi. “Excessive usage of job-searching websites like Glassdoor is tracked and marked. Even search words like ‘job’, ‘placement’, ‘career’, or phrases like ‘careers of an engineer’, are marked,” she says. You’ll either end up with a counselling session with HR or, worse, your promotion might be quietly blocked.

Don’t keep unsent emails

Have you saved the draft of a nasty mail to your co-worker or a resignation letter? Delete it urgently. “It is unlikely that the admin will read it, but it’s not impossible,” says Chandrachoodan. Most office laptops have admin software that can potentially check your drafts and downloads folder, or any information on the machine.

Delete personal files

Never save your personal files on a company’s cloud network, especially the ones you don’t want your boss, co-workers or the anonymous IT admin to see. Delete the medical report, the bank’s latest statement, the photos with your partner, or anything personal or sensitive. If you want to keep them on your company-owned device, keep them encrypted with a password, so that if anyone gets hold of them, they can’t access them. “Ideally, you shouldn’t do anything that is not related to your work on your company-owned device,” says Prasad Naldurg, a security researcher based in Bengaluru. “Use a personal phone or laptop, and keep your work and personal life separate.”

Ask before you download

Most company-owned devices come installed with a monitoring software that can review what is installed and whether it meets company standards. This software works in the background and logs your activity,” says Chandrachoodan. “If you try and install something that is problematic for the company and is not approved, it will either block your installation or raise an alert,” he says. As a rule, don’t install third-party software. If you need a software for a specific work, ask the IT department to find you the right one.

Resist the urge to rant

Want to head to Simply Confess (an anonymous social network) to gossip about your co-workers or the company, or write it all down in an anonymous blog? Refrain from doing it from a company-owned device, says Chaturvedi. “It’s a silly thing to do as the company servers have your browser history and they can easily find out who was the one on the specific site, at the specific time, bad-mouthing the company,” she says. The result, depending on how dire the deed is, could range from a reprimand to sacking.