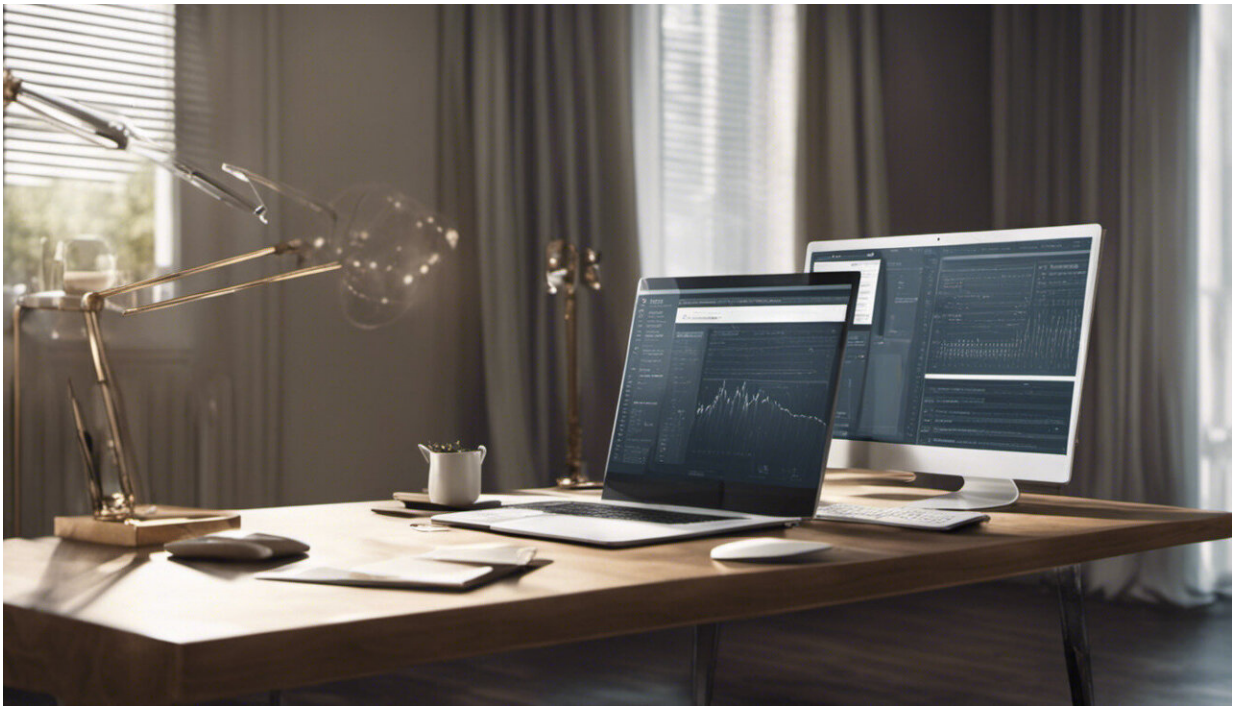
Working from home risks online security and privacy: How to stay protected

March 27 2020, by Jason Nurse



Credit: AI-generated image (disclaimer)

Remote working can be a blessing. More time with family, less commuting, and meetings from the comfort of your living room. But as millions across the world switch to working from home due to the COVID-19 pandemic, they may be putting the security and privacy of themselves, their families and their employers at risk.

Many will be using online collaboration tools, such as Zoom, Slack, and HouseParty to stay connected to colleagues and friends now that physical contact is restricted.

Zoom, the most popular of the video calling platforms, allows call hosts to track attendee attention, and in particular, whether you are in the Zoom window (as opposed to checking email or playing a game, for instance). Zoom also collects a host of other personal information such as each caller's location data, operating system, IP address, and what kind of device they're using, whether it's an Apple Mac, iPhone, Android or Windows device.

Zoom has had its share of security problems. A now-fixed software bug had allowed anyone to find and join a meeting. There was also a problem with its software which could have resulted in any malicious website turning on your camera and watching you unawares. And Zoom Bombing is now a thing. It involves trolls using Zoom's screensharing feature to display vile content, including violent videos and shocking pornography.

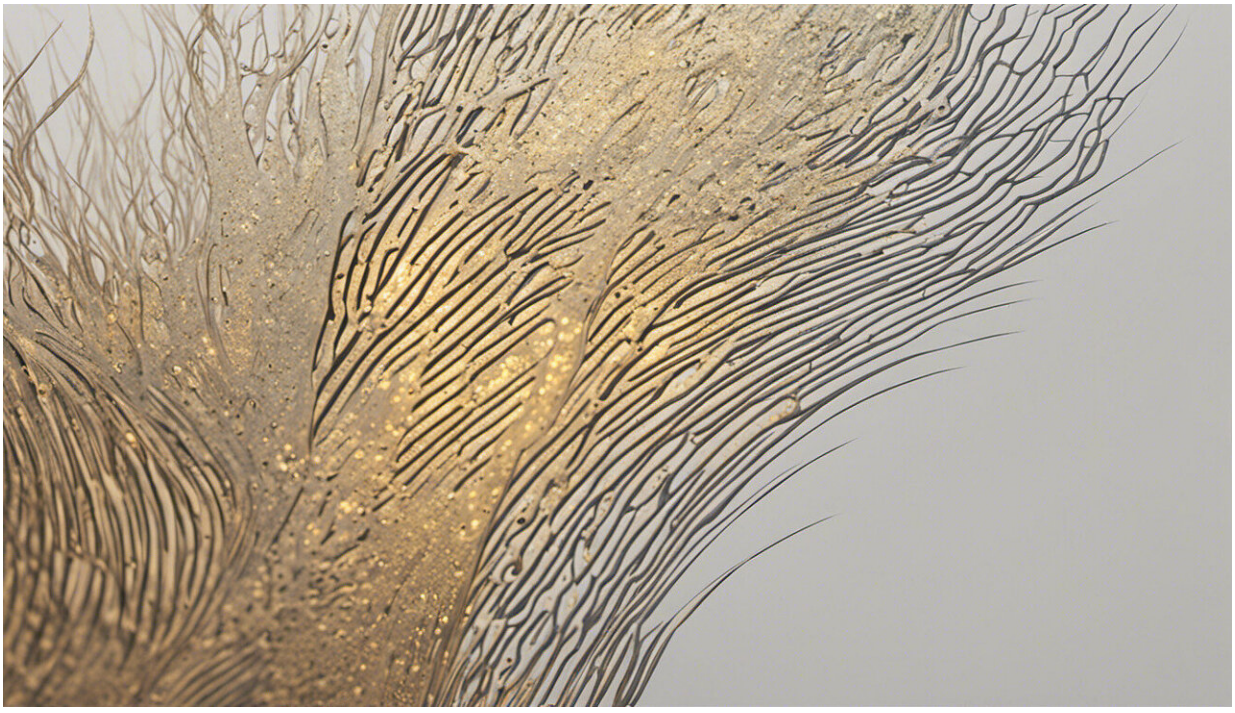
Another popular tool is Slack, which as it states, "is the place for remote work." A core feature of Slack is its channels. These are spaces to share messages and files with colleagues on particular topics and projects. While paid accounts have some control over how long their channel or private message data is kept by Slack, free accounts are much more limited. This could mean that your messages (including direct messages complaining about your boss or a colleague) are accessible to others, even if they aren't to you.

For many people, working remotely is a completely new experience. Some are celebrating the novelty by using the #WorkFromHome hashtag on social media, and sharing posts that include photos of home office setups, and friends and family members.

This may seem benign, but it can actually expose a variety of sensitive personal information about you and those around you.

For instance, posting photos of homeworking setups, which happen to include letters, post or Amazon packages, can publicize your home address. Sharing photos and names of family members or pets may provide hints about your passwords or even expose your location.

The now popular practice of sharing screenshots of Zoom work group chats or HouseParty video hangouts, also has its privacy risks, given the fact that companies have been known to indiscriminately gather the photos we share online and use them without our permission. This means anyone could match offline photos of us directly to our online profiles on Twitter, Facebook or LinkedIn. Some companies have even been known to use our photos in adverts.



Credit: AI-generated image (disclaimer)

Well-equipped cyber-criminals

Largescale remote working is a security nightmare for employers. As remote access to corporate networks is rolled out, cyber-criminals have their pick of places to attack.

Cyber-criminals are well aware of this, and have already begun to launch targeted attacks. According to the latest statistics, coronavirus-related fraud reports have increased by 400% in March alone. There have been scams for COVID-19 tax refunds and others impersonating the Centre for Disease Control to request donations.

Criminals have impersonated staff from the World Health Organization (WHO) and there have been extortion emails that threaten to infect recipients with coronavirus unless they pay up. Even coronavirus outbreak and infection-tracking maps are being used to spread malware.

These problems are made worse by the reality that many of us will be using personal, and potentially less secure home devices, such as laptops, phones and USB drives, for work tasks. Most people aren't accustomed to maintaining workplace security practices over long periods in our homes, with kids, distractions and other commitments.

How to stay safe

- Be careful what you post publicly. Check that there is no potentially sensitive information in it. Once it's published online, it's there, forever.
- Check recent security and privacy reports about online collaboration tools before using them, and if in doubt, consult your employer. These tools can have access to details about your

devices, your data and your video and audio conversations. The Electronic Frontier Foundation is a good source.

- Protect your devices. Install anti-virus software, update systems and apps, implement multi-factor authentication (so that multiple pieces of evidence are needed for someone to use your login, such as username and password and a text message), and be on the lookout for phishing scams.
- Zoom Bombing and other forms of hijacking meetings can be prevented. Share meeting links with only invited parties. Configure Zoom to only allow the host to share screen, as appropriate. And disable file transfers to stop trolls sharing viruses to all attendees.
- More tips are available through the WHO, WEF, NCSC, ENISA and FTC.

Provided by The Conversation

Citation: Working from home risks online security and privacy: How to stay protected (2020, March 27) retrieved 12 August 2024 from https://techxplore.com/news/2020-03-home-online-privacy.html