Last week Instagram hit 500 million active users and in commemoration Zuckerberg posted the above photo to his Facebook page. Mark had inadvertently revealed three things:

1. That his Mac camera is covered with tape.
2. That his Mac microphone is covered with tape.
3. That his email client is Thunderbird.

Mark Zuckerburg is clearly worried about his cyber security – he is a high value target who has been hacked before – so instead I'm writing an article about the steps that Mark Zuckerberg takes to protect his privacy and why security experts think we muggles should all do the same.

Why you're at risk

We live in an age of ever increasing connectivity and reliance on technology. At the same time, and as a direct result, we also live in an age where the NSA has the power to monitor emails and text messages sent by the American people. Not to mention the ability to secretly tap into hundreds of millions of Google and Yahoo accounts worldwide, where nearly one million new malware threats are released every day and where hacking costs the global economy an estimated $575 billion on an annual basis.

So yes, if you have a computer, if you use a phone, if you use email, you are at risk of being hacked.

While it might be easy to conclude that Mark Zuckerberg is your garden variety paranoid, eccentric, billionaire when he tapes over his laptop's microphone and camera, in reality he is protecting himself against a risk that we all face.

Zuckerberg is protecting against "ratting" - slang for a Remote Access Trojan cyberattack. A RAT is a form of malware which can give a hacker remote control of your computer – including your webcam and microphone.

Today the risk of this kind of attack is high – 70 percent of malware consists of Trojans and the most easily deployable of these is the RAT whose source code often only costs $10 to $50. Hackers can use this control to do a wide range of bad things to you:

- Hijacking control of personal computers.
- Watching and logging your keystrokes
- Downloading, uploading, or deleting files
- Destroying your CPU through overclocking
- Installing additional viruses and worms
- Editing your Windows registry
- Using your computer for a denial of service attack and to otherwise infect friends and family
- Stealing passwords, personal identification information, and credit card numbers
- Wiping your hard drive
- Installing hard to remove boot-sector viruses

And even to spy on victims through remote control of webcams and microphones.

In 2014, a website opened that played live video from ***thousands*** of webcams in over 250 countries.