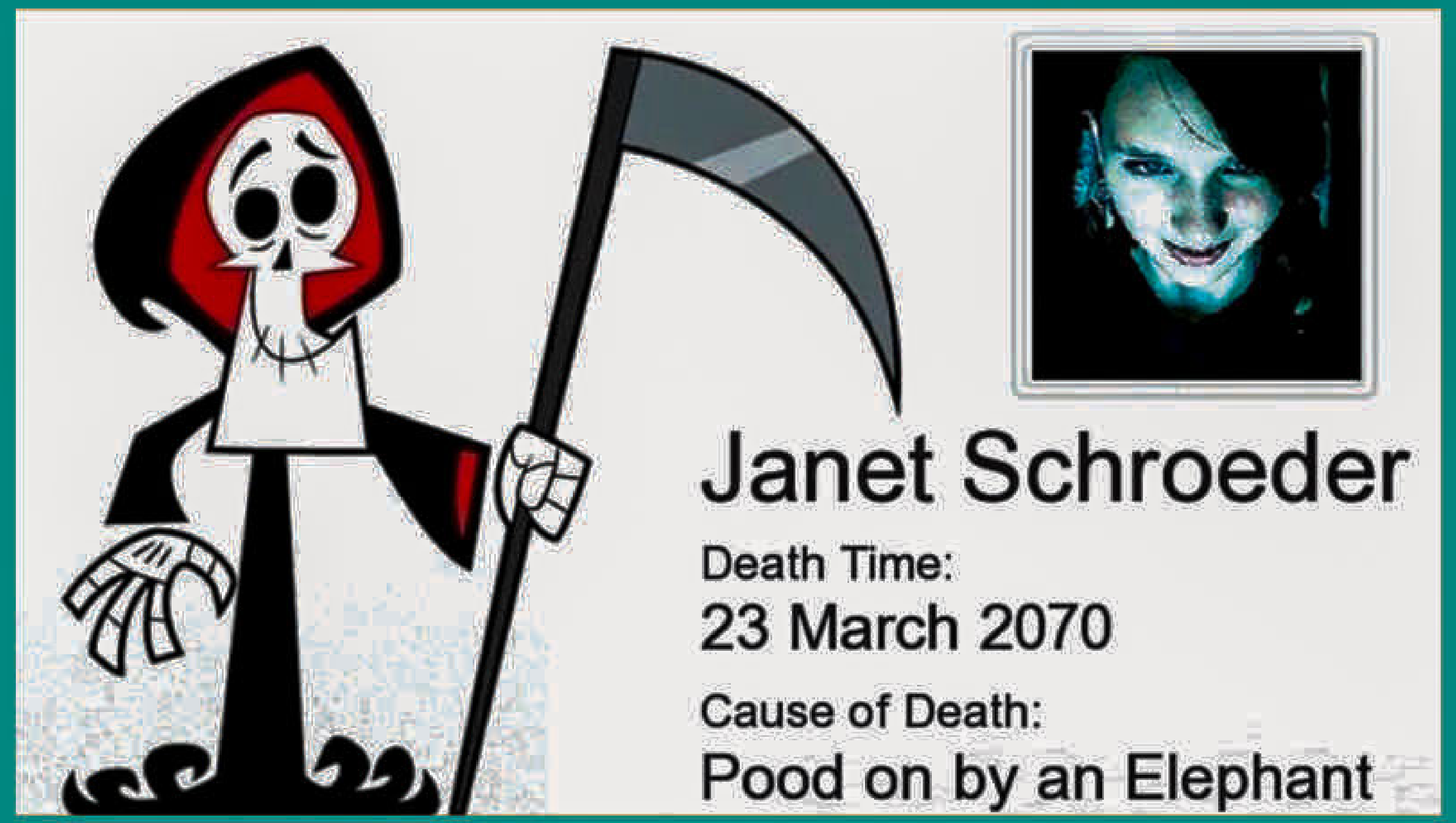
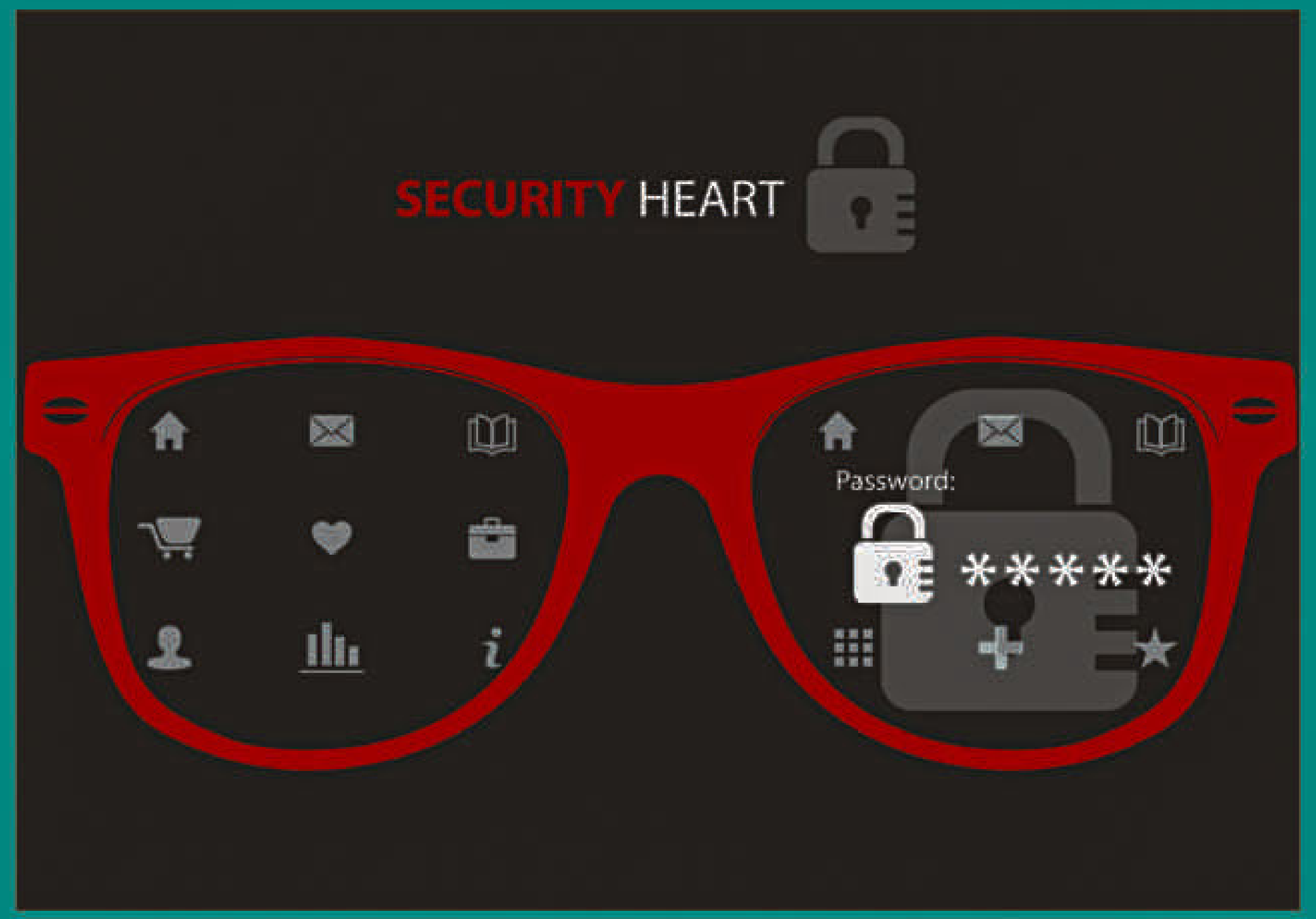
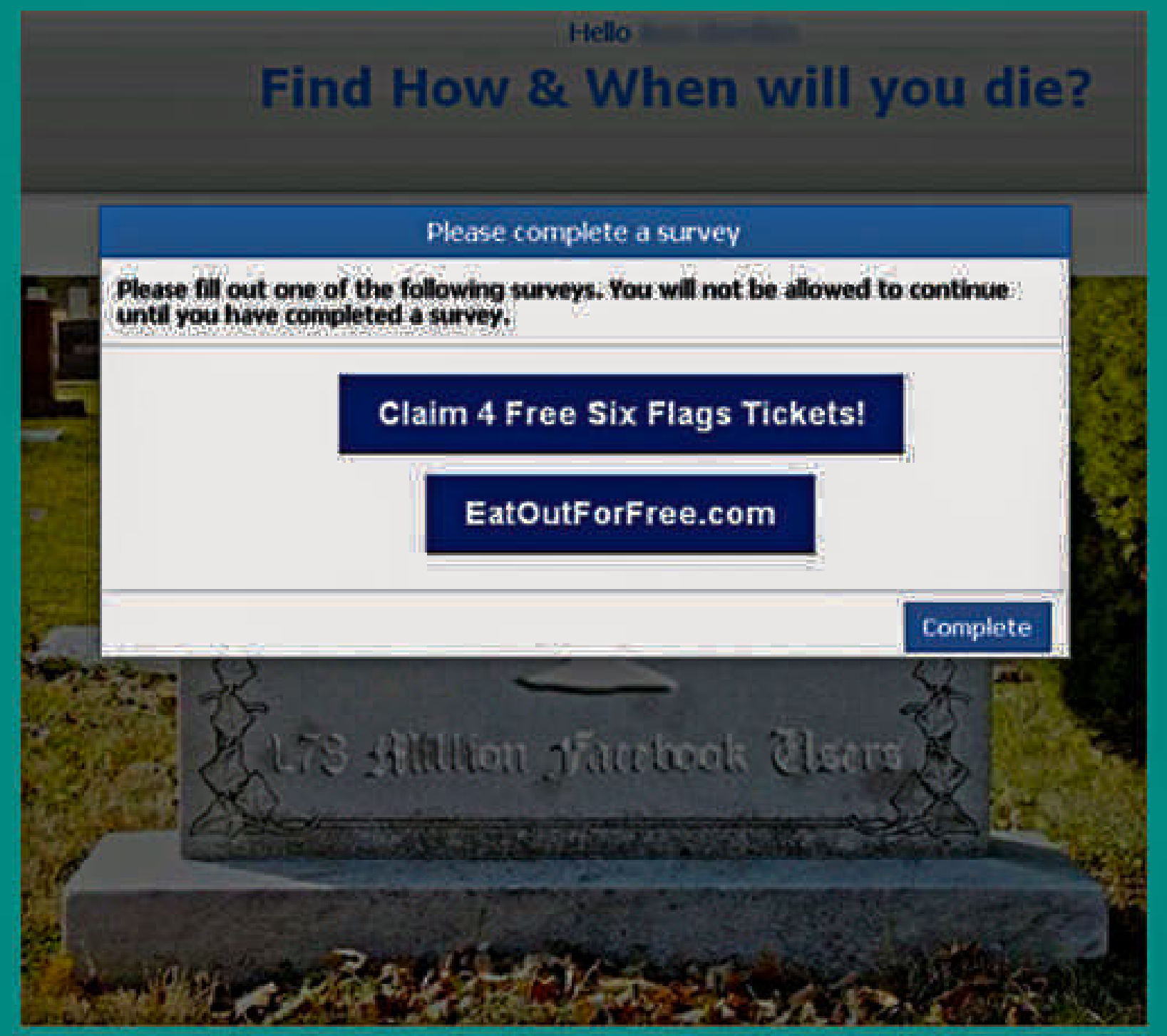
Why the Internet is not as safe as you think

THE DEFINITIVE YOUTH MAGAZINE SHOUT






Hello

Find How & When will you die?

Please complete a survey

Please fill out one of the following surveys. You will not be allowed to continue until you have completed a survey.

MITHI CHOWDHURY & SARAH ANJUM BARI

There's little doubt that nothing has shaped the world more radically than the Internet. The most significant of its impacts is how it has created a need in everyone to have an online social presence, which brings with it both benefits and hazards.

Our news feeds today display increasingly shared excerpts from Humans of New York or berlin-artparasites. In both instances, we read about complete strangers from starkly different backgrounds, cultures and even time periods and yet, we connect with them. While the influx of information – from European refugee crises to the latest sale on ebay – keep us connected to the world, constructive online communication and planning by the youth have recently helped battle significant issues such as the 'VAT on education' movement in our own country.

One only needs to look through the 'Other' section of Facebook inbox to get a glimpse of the sexually offensive messages women receive every day. "Ignore it." – that's what women are told. Never mind that these messages are no different from the barrage of vulgar remarks we hear while crossing the Farmgate overbridge every day.

All this is testament to what an internet presence can accomplish.

Sceptics talk about how social media is a threat to people's security and privacy. It's easy to say that they fail to understand how the same is true for all things of power. Something that has the strength to change and mend issues of the world can also be mishandled to cause harm.

Like any burgeoning metropolis, the Internet too has neighbourhoods – some safe while some are akin to the sinister Elm Street. In spite of all the precautions we take to safeguard ourselves against this unaudited entity – filtering softwares, pre-filtered internet providers, and innumerable firewall configurations – it's in our nature to disregard the very boundaries we create to protect ourselves. We frequently lie about our identities, location or even family background – it seems to be an almost banal side effect to our addiction. Anonymous comments that tear your self-esteem to shreds are routine, and it's not a normal day if you haven't been confronted by harassing messages online.

Farhan Shahriar, a student of Adamjee Cantonment College, had his Facebook account hacked recently. "The hacker blocked all my close friends and started adding random people," said Farhan. When asked how the incident made him feel, he said, "Initially, I felt quite scared because I thought my account would send irrelevant messages to strangers using my name. Other than that, it was okay. It was just my Facebook profile, not my bank account."

Among the many cases of cyber attacks we've reviewed, the general consensus seems to be: *These things happen*. One only needs to look through the 'Other' section of Facebook inbox to get a glimpse of the sexually offensive messages women receive *every day*. "Ignore it." – that's what women are told. Never mind that these messages are no different from the barrage of vulgar remarks we hear while crossing the Farmgate overbridge every day.

Unfortunately, this is the harsh reality of life online. We've become so desensitised to cyber assaults that it takes something truly horrific to really grab our attention.

Dristy Rahman, a victim of cyber-harassment, made sure her profile had strict privacy settings activated, but found fake accounts to her name nonetheless. The accounts were supposedly used to ask strangers for money. Eventually, other users (who also appeared to be using fake accounts) posted on the DSD Facebook Page, complaining of having been conned by her. With her name and photographs attached to the incriminating accounts, there was no way for Dristy to avoid embarrassment.

When asked how she resolved the matter, Dristy explained, "When I went to the police station to file a report, I was told that there were thousands of such cases and it is quite difficult to track down the culprits. My friends – and other connections I have – made sure that the posts were brought down. We reported the accounts and also posted on every Facebook group possible, advising the members to act similarly if the accounts resurfaced. After two days of constant watch, it stopped."

"There are still many fake accounts using my pictures, but with different names. The same happened to one of my friends. She was even about to be arrested," Dristy added.

However, dealing with these incidents goes far beyond having them removed from the public eye. Once something is made visible online, it stays on in the form of screenshots or word of mouth. Even if it's deleted, the shame of public humiliation isn't easy to get over. "I cried throughout the entire night when I first found out," shared Dristy.

"Then, my mother pointed out that my friends and family know me regardless of what is posted online. I couldn't have overcome this without my family's support."

It's easy to believe that these are isolated incidents but reality begs to differ. Social media affords these delinquents anonymity and unaccountability, leaving victims with a crippling sense of helplessness. How do you confront an anonymous, faceless perpetrator?

Social media affords these delinquents anonymity and unaccountability, leaving victims with a crippling sense of helplessness. How do you confront an anonymous, faceless perpetrator?

As we continue to wait for a legal system that protects victims of cyber assaults, it's paramount that you learn to protect yourself. Here are a few ways through which you can ensure your safety –

1. Trim out your friend list, refrain from chatting up strangers and allowing them to view your Instagram posts or Snapchat stories, and avoid posting frequent 'check-ins'.

2. Choose a strong password. No, *password* doesn't count. Longer words are generally harder to guess, so opt for those. Also, try substituting alphabets for numbers.

3. Give passwords that are significant only to you. For example, if the name of your first childhood pet was SirWoofs-A-Lot, reconstruct it into something unique like S!r3oof454.

4. Checking the URL of a content or website is a great way to ascertain whether that particular site is safe or not – such as *"getmoneyfast.com"*. Sounds like an identity-phishing website? That's because it probably is.

5. Always check the email address. Many senders of scam emails won't have addresses that match the company they supposedly represent. The addresses will be slightly altered so as to avoid detection.

6. On Facebook, do not give random apps like *"Which Harry Potter character are you?"* permission to view your personal information. Many hackers use badly designed apps with catchy titles to gain access to your profile.

7. When collecting security question, choose harder ones with answers that can't be figured out from your social media profile.

8. A firewall is software that creates a barrier between your network and the external cyber world, allowing only certain data to reach you. Install a third-party software programme of your choice.

9. Secure URLs begin with *https://* instead of *http://*. This means that the transmission is encrypted to and from the web server.

10. Another necessary step, but one that we tend to overlook, is to stay up-to-date on the safety features of social media sites. Skim through the privacy updates of Facebook, Snapchat, Instagram and other sites, no matter how tedious it might seem.

Most importantly, NEVER give away personal information (ESPECIALLY online), such as passwords – not even to friends or family. Their accounts may be hacked without their knowledge. Remember, prevention is always better than the cure.