

*JEROME OKOT - Chief Operations Officer, Milima Security*

As we speak right now, 50% of the world's total population is active on the internet with over a quarter of the population using Facebook. Also, as we speak there is 5million and more google searches taking place right now. See for yourself here <https://www.internetlivestats.com/> What is hard to notice is how much information is being given away, later on traded with or without our consent. This brings us to the idea for this newsletter.

A digital footprint is a trail of data one creates as they use the internet. Whether it's simply a google search, a text message, or shopping activity. It is a trail because most of it is recorded with our consent and sometimes sadly, without! How much of your information is out there, does it identify you, and most importantly, is it secure? Statistics show that as of January 2019 there are 2,579,000 Facebook users in Uganda. This accounts for 5% of the total population of the country (<https://bit.ly/UGfbStats>). With the fast evolution of technology and increased internet penetration post covid19, this number will be even bigger by end of 2021.

We often volunteer information as we use the internet, and forget to keep track of it. Sometimes we have shared Personally Identifying Information (PII), and endangered ourselves, and even the people we love. How bad is it to be this exposed? Watch this [https://www.youtube.com/watch?v=Ro\\_LlRg8rGg](https://www.youtube.com/watch?v=Ro_LlRg8rGg). Some of the risks we are exposed to by an insecure digital footprint are data exposure, domain threats, impersonation, phishing and others.

For organizations, the task of protecting the digital footprints of employees is difficult because a company is the sum of its employees, and each worker has their own digital footprint. Using these "digital breadcrumbs" and connecting the dots between all these publicly available details can significantly extend the attack surface over a company.

This is how hackers use publicly available employee data to illegally access company systems.

The following statistics as mentioned by the Security newspaper are interesting;

- 45% of people publicly disclose their birth date
- 29% share their phone number on the Internet
- 20% share their address
- 14% mentions their mother's maiden name
- 7% share their social security number online

We can cause as much trouble by not securing our traces on the internet and also, we can easily get our reputations trailed and cloned or even damaged.

How might we ensure that we are safe on the internet? It is of course prudent to ensure best web browsing practices among other means such as these, according to Norton;

1. Enter your name into several search engines.
2. Double-check your privacy settings, but don't trust them.
3. Create strong, memorable passwords.
4. Keep all your software up to date.
5. Review your mobile use.
6. Build your reputation through your behaviour.

Managing digital footprints requires a constant effort since Web tools are constantly being launched, and it is important to be updated. The high internet penetration levels have increased the available data which makes it easier for hackers to search for key information to access their targets.

Cleaning your fingerprint is a necessary practice in today's world, so relationships must be built with specialists in data privacy and protection services, so they could not suffer bad security experiences due to the digital footprints left online. Milima Security has a course on Data Privacy and protection that could come in handy. Check here <https://www.milimatechnologies.com/> and inquire even for some advisory. Consider calling or texting(WhatsApp) directly using +256778290491.

Know your digital footprint but most importantly, protect it. It can make or break you!