Why Cybercriminals Love the Work-from-home Era

Technology, Privacy, and eCommerce

Photo By Golden Dayz/Shutterstock.com.

Working from home is here to stay, at least some of the time. But it has opened the floodgates to cybercrime. Syngenta's automated firewall blocks more than 30,000 suspicious email activities every day. And last year there were 1.8 million cyber-attacks on home networks – almost 5,000 a day.

The good news is that there are quite a few simple habits we can build to protect ourselves while working remotely, using home Wi-Fi, or a mobile hotspot.

Several of our Syngenta experts recently sat down for a discussion and created a list of key tips.

Avoid the phishing trap

You receive an email asking you to fill in a form or click on a link. It looks and feels very similar to any normal email, but it is someone maliciously trying to steal your identity or gain confidential business information.

For example, in India, colleagues received an email supposedly from Human Resources, with a Syngenta email address, sent at 5:30 a.m., asking them to update certain data. Looking closely, the email address was not standard for Syngenta. And HR does not send out emails at 5:30 a.m.!

The best way to spot these emails is to be vigilant. Look closely at the email address of the sender – does it seem genuine? Do any attachments look normal? Are the links to URLs ones that you would expect? If you're concerned, report it to your organization's IT team or tell your manager.

Good habit: Think before you click, look before you act.

Store and share data safely and legally

Unlawful loss or disclosure of data can have serious consequences for individuals and Syngenta as a "data controller."

Avoid hoarding data. Typically, we save data for a rainy day. You may think it is harmless to keep old documents on your laptop. That isn't the case – if your system is compromised, and old data leaks out, it could still cause harm.

> You may think it is harmless to keep old documents on your laptop. That isn't the case – if your system is compromised, and old data leaks out, it could still cause harm.

Most data shouldn't be needed for more than six months. Where data may be needed for litigation, it can be stored for longer. A good legal department should flag potentially litigious data. Private SharePoint or Teams channels are one way to save data without keeping it on your laptop.

Data breaches often come down to simple human error – which of us has not sent an email to the wrong person? Another potential risk is sending work-related information via a personal email or through non approved third-party vendors that facilitate the sharing of large amounts of data.

Documents attached to emails should always be encrypted or password protected.
Here's how-to-encrypt a document:

In the document, click on the right button of the mouse, select 7-zip, then add to archive, and in the encryption section, add the password. After that, remember to send the password to the recipient by a different email or channel.

Good habit: If you don't need it, don't keep it – declutter!

Secure your home Wi-Fi network and devices

Our home Wi-Fi has suddenly become our best friend but exposes us to a world of threats. Strong passwords are one great defense. Did you know: It takes 8-10 seconds to break a password with simple ABC or 123 characters, but millions of years to break a complex 14-character password?

> Did you know: It takes 8-10 seconds to break a password with simple ABC or 123 characters, but millions of years to break a complex 14-character password?

Keep your devices up to date with the versions and the patches that you have available from the company side. Otherwise, devices become vulnerable.

Use VPN whenever you can, not only when you are using home Wi-Fi but – if possible – while using a mobile hotspot.

Working on the train? Beware of “shoulder surfing, “when a malicious individual sees your screen and steals information. Use a privacy screen, either a digital one or a physical screen.

Good habits: Create strong passwords, always update your devices, and use VPN and a privacy screen, when needed.

Check out ACC?s Resource Library.

Helena Sousa Aguiar

Global Data Protection Office Manager

Syngenta Group

Helena Sousa Aguiar is the global data protection office manager for Syngenta Group. She joined Syngenta in 2021, following three years of General Data Protection Regulation (GDPR) implementations across several sectors and industries leading a team of eight, working closely with cybersecurity and compliance teams. Aguiar is certified with the International Association of Privacy Professionals and as a lawyer and barrister with the Portuguese Bar Association, since 2012 with international taxation background. Aguiar supports the Syngenta Group's response to an ongoing and rapid expansion of a new global data protection regulatory landscape across the globe.