BLOCK THE HACK

The digital world is all-encompassing and nothing can quite match up to it in terms of convenience. However, there are certain pitfalls we must watch out for

By **Bindu Gopal Rao**

GETTY IMAGES

Today everything is digital, from bank transactions to stock investments to making payments and even sharing memories. While all of this is convenient and seemingly happens at the click of the button, it is important to realise that you are not alone and are likely being "watched". Well, to put it in simple words, the cyber world is full of hackers that are looking to siphon money and stealing information that can cause a huge dent financially and otherwise. Again, this problem is magnified in high networth individuals (HNIs) because of their wealth. According to www.cybersecurity-insiders.com about nine Mayfair art dealers/galleries in UK have lost almost €1million to hackers through an email scam. "The probe discovered that the methods are simple. Cyber crooks gained access to the art dealers email ids and continuously monitored their emails in and out. When the art galleries sent PDF invoices to clients, hackers sent a duplicate invoice impersonating galleries email address and told client to ignore previous invoice and instead wire payment to the bank account mentioned in the second invoice. The same technique has been used by the hackers to steal money paid by galleries to artists," says Mimi Partha Sarathy, Managing Director, Sinhasi Consultants Pvt. Ltd.

STAY SAFE

Naturally, HNIs must ensure they protect themselves against cyber threats and using multi-factor authentication is key. "For years, we have done what our IT overlords have told us to do - use strong passwords, and change them often. But passwords are only one factor and the most common implementation of one of the three factors. The factor of "What you know" is the first. The computers we have traditionally used require only that one factor. The second factor is "what you have." In other words, this factor uses tokens. If you have ever been sent a text token via your mobile number to help reset a password or log in to a system, then you've used this second factor. The third factor is, "What you are." This third factor is implemented through biometrics. If you have an Apple iPhone that uses

face recognition, you're already implementing this "what you are" factor. In the future, try to implement at least two of these factors for more security," advices Dr. James Stanger, Chief Technology Evangelist, CompTIA. Keep the focus on doing simple things like setting some time aside one day a week to monitor credit card statements and bank statements to locate and take necessary action if anything suspicious. Zakir Hussain - Director, BD soft, Country Partner of Bitdefender opines, "HNIs can secure their gadgets by securing an account through Automated System which works on keeping multiple back-ups of the important data and is also certainly worth it. But one always should choose secure and trusted channels to connect to their Corporate Infrastructure or Internet viz. VPN & Secure Trusted Wi-Fi Zone. Doing so could prevent unauthorised accesses. Many Market Software Companies have also launched their own endpoint multilayered security products, for example, antimalware, antispam, anti-phishing and strong content filtration solutions. These solutions are a boon to prevent cyber-threat."

> Keep the focus on doing simple things like setting some time aside once a week to monitor credit card and bank statements to identify and take action against anything suspicious

TOOLS & TECHNIQUES

In order to equip yourself to counter cyberattacks, you can train yourself with simple one-hour videos and safe computing practices that are usually not part of everyone's everyday thinking. "Training even if it's video-based can help ensure that safe computing practices become automatic. It is important

TIPS FOR ONLINE SECURITY

- Change your passwords frequently at least monthly and never write down the password anywhere.
- Use a strong password and follow the instructions of the service that requires you to create the password. Do not use your date of birth or pan numbers as your password.
- Never use the same password across multiple services, especially any financial services (e.g., your bank).
- Do not connect to unknown wifi networks and download new software only from trusted, verified sources.
- Avoid being distracted as you work.

to make security part of your "muscle memory." We have a product called CyberSecure, for example, that is quite effective. Also use password vault software. For example, if you still have to use only passwords, you will have many passwords to manage. Use a password manager. I call it a "password vault." But if you use a "password vault," you can manage them much more easily. Examples of password vault software include LastPass, Zoho Vault, Dashlane and LastPass," says Stanger. Bitdefender redesigned the products which used the common infrastructure such as operating systems supported by Linux, Windows, Mac, Smartphones, and Tabs. The latest adaptive technology provides best security and technology; likewise benevolence the Multi-layered security works against all cyber-threats.

TECH TALK

In today's world the operative word is mobility as we are all on the move with mobile devices that often makes it very easy for attackers to discover your location and if you were away from home. Again it is easier for hackers to find you as you travel and wage some form of attack. "We have more devices available to us than ever before. This fact alone has created a large "attack surface" for each individual. At one time, we may have had one or two networkable devices on our persons. Now it is many (watches, tablets, phones, gaming devices, notebook PCs). The more devices we have on us, the easier it is for someone to exploit a weakness. Each device contains dozens, if not hundreds of applications. Some of these applications could very easily have serious security issues." This is why there is a need to use new age technologies to ensure that novel threats can be combated. "In the new iPhone, face recognition is a new technology that enables multi factor log in. Most commercial grade handheld devices or laptops come with fingerprint identification system. Password manager programmes compel users to set strong passwords and also send schedules to figure out the time when passwords must change. These programmes can be used on multiple devices and different mobile platforms. Privileged Access Management (PAM) involves the use of special software that can better and more securely track a user's login session and identify anomalies and, possibly, malicious behavior," explains Stranger. So it is time to sack the hack and control your safety online. M