Cyber Risk And Digital Fingerprints

cyber security risk management

Summary: Cyber criminals can now replicate digital fingerprints. We provide you with some tips to stay safe.

Forbes research finds there are things you should not say at work, if you want a great career. These include: "It's not fair"; "This is the way it has always been done"; "No problem"; "I am going to ask a stupid question" and "This will only take a minute."

While some things shouldn't be said at work, others are important to share with all employees. One instance of this is when it comes to phishing scams and even stolen fingerprints; there is no shortage of tactics criminals employ.

If you think you have seen it all though, think again. Criminals no longer need people's actual fingerprints in order to impersonate them and gain access to sensitive information. Instead, they are able to breach security and gain access by replicating what are known as the "digital fingerprints" of computers and mobile devices.

That's right--just as no two humans have the same fingerprints, the digital fingerprints recorded by people's individual devices are unique and stored by digital systems. Things like user behavior, IP addresses and operating systems are unique and are used by security systems, as a means of verifying an identity. Naturally, cyber thieves have now figured out how to steal and take advantage of these digital fingerprints, as well.

According to a new report from intelligence company IntSights, hackers can now use everything from a person's Facebook habits, to their web surfing patterns to impersonate that individual so well that they are able to get past advanced identity protection systems to gain access to accounts.

That is spooky, and since it is not uncommon for people to save login credentials on their browsers, there is an almost limitless amount of information hackers are able to exploit, once they start getting their hands on such data.

Having first sprung up in November 2018, a marketplace called Genesis began offering digital fingerprints for sale and a second marketplace named Richlogs, which offers even more comprehensive information than its predecessor, sprang up in April. Through these marketplaces, criminals can purchase an individual's digital fingerprint for between $200 and $250, depending on how much information is stored in the cache of that person's computer.

To take active steps on this security front, there are a number of things you can do. First, continuously monitor digital identity markets for the possibility that the digital identities of any customers or employees have been compromised. For financial institutions that use actual digital fingerprinting as a security measure, it is crucial to routinely update such protocols.

Multi-factor authentication is another important security measure that can be used, as requiring mobile verification or unique security questions makes it more difficult for hackers.

Lastly, encourage both customers and employees to regularly change passwords and remind everyone to frequently clear the cache on computers to remove cookies and browsing history. Stay safe out there!

ON DEMAND HELP FOR FINANCIAL INSTITUTIONS

Financial institutions face many difficult challenges every year, but you are not alone. Our experts stand ready to help you address a variety of issues. Find out more about our solutions today.