Security Newsletter

31 July 2017

Sweden Accidentally Leaks Personal Details of Nearly All Citizens

Swedish media is reporting of a massive data breach in the Swedish Transport Agency (Transportstyrelsen) after the agency mishandled a deal with IBM, to outsource database and IT service management. IBM, which in turn outsourced the operations to countries in eastern Europe, with the result that “foreign staff had responsibility for Swedish classified information”.

What’s do we know about what’s been exposed? The agency has information on all vehicles in Sweden, including some, but not all military vehicles. It also is the depository for the nation’s driver’s license data, including photos – which also happens to include individuals under protective order, and those of undercover law enforcement workers. Additionally, the nation’s infrastructure data with respect to roads, ports, air, rail, etc., is under its sway

Although the data breach happened in 2015, Swedish Secret Service discovered it in 2016 and started investigating the incident, which led to the fire of STA director-general Maria Ågren in January 2017. Ågren was also fined half a month's pay (70,000 Swedish krona which equals to $8,500) after finding her guilty of being "careless with secret information," according to the publication. What's the worrying part? The leaked database may not be secured until the fall, said the agency's new director-general Jonas Bjelfvenstam. The investigation into the scope of the leak is still ongoing.

The Swedish prime minister has admitted that the leak of the confidential data of millions of Swedes as a result of the country’s transport agency outsourcing operations to third party contractors is “a disaster”. Speaking in Stockholm on Monday, Stefan Löfven also confirmed that he had known about the leak since January, with other ministers being aware of it as long as 18 months ago

Read More

Even More

Passwords Evolved: Authentication Guidance for the Modern Era

In the beginning, things were simple: you had two strings (a username and a password) and if someone knew both of them, they could log in. Easy.

A couple of months ago, Troy Hunt wrote about Password reuse, credential stuffing and another billion records in Have I been pwned (HIBP). That presents a very interesting challenge: how do we defend against this? I mean you're trying to run your online system and someone has valid credentials for some of your users, how are you going to stop them from getting in? The simple string matching of the 60's just isn't going to cut it.

There's a lot more to how authentication has evolved than just the rise and rise of credential stuffing though, many other aspects of how we logon to systems has also changed. In some cases, this has led to once-held "truths" about how we create and manage accounts to be totally flipped on their head, yet we still see modern organisations applying the patterns of yesterday to the threats of today.

This post tries to address this gap and talk about how we should be designing this critical part of our systems today. Hope is that in times where a company says "we're doing this screwy thing because security", this post becomes a resource that well-wishers direct them to.

Read More

How To Protect Your Users With The Privacy By Design Framework

In these politically uncertain times, developers can help to defend their users' personal privacy by adopting the Privacy by Design (PbD) framework. These common-sense steps will become a requirement under the EU's imminent data protection overhaul, but the benefits of the framework go far beyond legal compliance.

PbD has existed as a best-practice framework since the 1990s, but few developers are aware of it, let alone use it. That's about to change. The EU's data protection overhaul, GDPR, which becomes legally enforceable in May 2018, requires privacy by design as well as data protection by default across all uses and applications.

As with the previous EU data protection regime, any developer serving European customers must adhere to these data protection standards even if they themselves are not located in Europe. So, if you do business in or sell to Europe, privacy by design is now your responsibility.

This presents a monumental opportunity for developers everywhere to rethink their approach to privacy. Let's learn what PbD is and how it works.

Read More

Biometric Authentication Overview, Advantages & Disadvantages

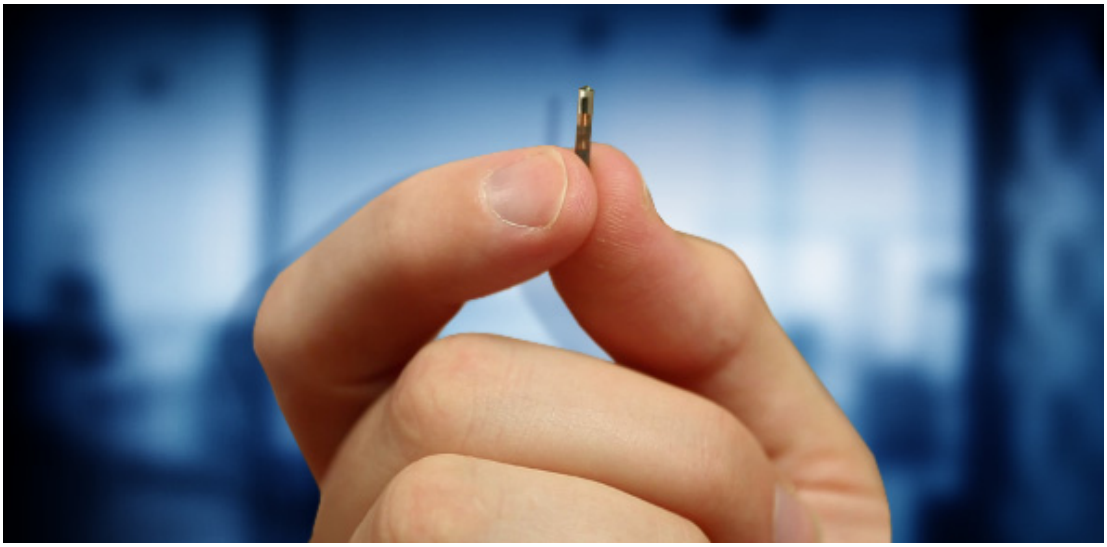
Biometric authentication works by comparing two sets of data: the first one is preset by the owner of the device, while the second one belongs to a device visitor. If the two data are nearly identical, the device knows that “visitor” and “owner” are one and the same, and gives access to the person.

Biometric seem to be everywhere these days. Consumer preference has turned the technology into a must-have for the modern smartphone or laptop. Fingerprint readers, face recognition or iris scanners are the most immediate examples, but researchers and engineers want to create even more clever solutions such as voice recognition. Some methods are pattern based and learn how you hold your phone or type at a keyboard.

Whichever way you look at it, the tech is here to stay. The real question however is, how effective is biometric authentication when it comes to keeping you safe?

Read More

32M Becomes First-Ever Company to Implant Micro-Chips in Employees



A Wisconsin company is offering its employees the opportunity to have a microchip implanted in them. The microchips utilize Radio-Frequency Identification (RFID) technology, which can identify nearby electronically stored information through electromagnetic fields — much like contactless credit cards and mobile payment systems.

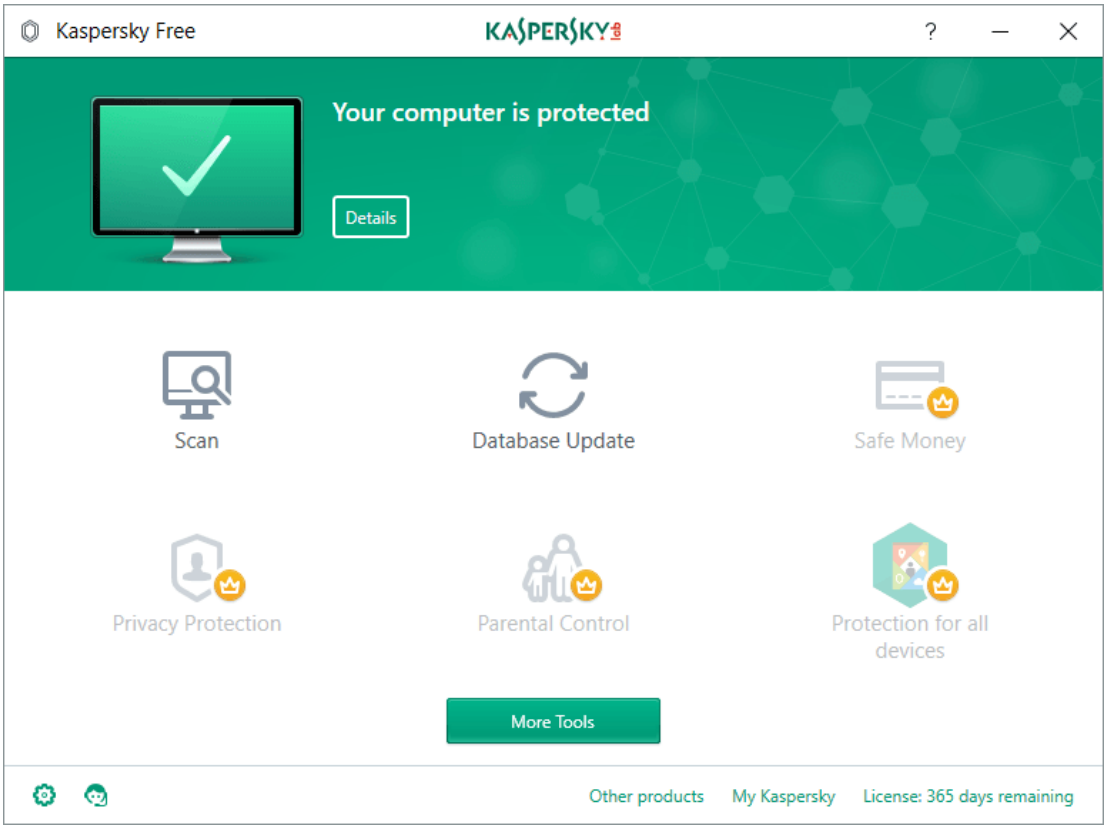
More than 50 employees are expected to have the chip lodged into the area between the thumb and the index finger. Not only does 32M want the microchips to eventually be used for accessing secured rooms and activating printers, it also hopes it can be used for making purchases at their software powered kiosks.

While the Biometric information and technology are experiencing an increase in popularity, it also raises widespread concerns around the safety and privacy of people adopting it. Hackers could misuse the technology used to provide easiness to the public against the public itself, and one should not forget that with the advance in technology, the techniques used by cyber criminals also improves.

Read More

Even More

Kaspersky Lab releases free antivirus software in global push



Amid every increasing suspicion that Kaspersky is in bed with the Russian government, comes the launch of Kaspersky Free – a free version of the software that was made available across the globe immediately. The free version of its anti-virus software is now available in United States, Canada, and several Asia Pacific countries with it being launched in the remaining territories in the coming months.

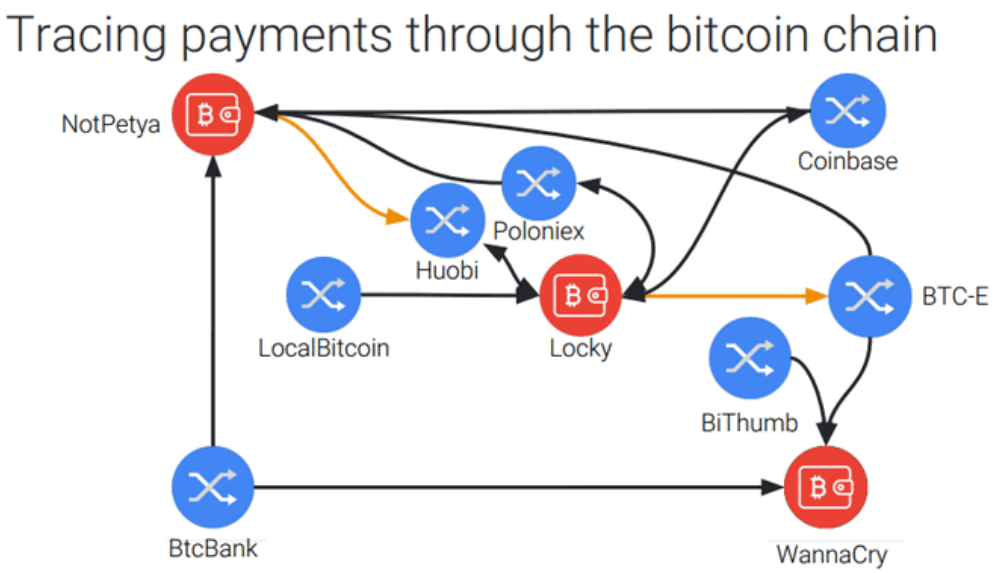
Kaspersky has said that the free version of its security software is not meant to act as a full fledged anti-virus solution since it only offers the bare essential features like email and web antivirus protection and automatic updates and lacks VPN, Parental Controls and Online Payment Protection.

Founded in 1997, the company has grown into becoming one of the top anti-virus software companies in the world. Through this rise though,the company has also faced questions regarding their relations with Russia's Federal Security Service or FSB (the successor to the KGB). Maybe the launch of a free version is the company's attempt to win back some of the lost faith.

Read More

Official announcement

How Hackers Cash Out Thousands of Bitcoins Received in Ransomware Attacks



Digital currencies have emerged as a favourite tool for hackers and cyber criminals, as digital currency transactions are nearly anonymous, allowing cyber criminals to use it in underground markets for illegal trading, and to receive thousands of dollars in ransomware attacks—WannaCry, Petya, LeakerLocker, Locky and Cerber to name a few.

It's obvious that after ripping off hundreds of thousands of cryptocurrencies from exchanges, wallets and ransomware victims, cyber criminals would not hold them in just digital form—the next step is to cash them out into real-world money. According to a recent research paper presented by three Google researchers, more than 95% of all Bitcoin payments collected from ransomware victims have been cashed out via a Russian cryptocurrency exchange, called BTC-e, since 2014.

Interestingly, just two days before Google presentation, one of the founders of BTC-e exchange, Alexander Vinnik, was arrested by Greek police on charges of laundering over $4 Billion in Bitcoin for culprits. The cryptocurrency exchange is believed to have been involved in cashing out Bitcoins stolen from the once-very popular Japanese bitcoin exchange Mt. Gox, which was shut down in 2014 following a massive series of mysterious robberies.

Read More

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with over 15 million customers across 100 markets. We offer pre-game and live Sports betting, Poker, Casino and Games through 13 subsidiaries and brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and as an innovation driven company that builds on trust.