**Could Your Smartphone Be Hacked?**

Here's the problem we're always running into with technology: In order to get something, sometimes you have to give something up. So, while more than two billion (more than one in three) people now own a smartphone that allows them to walk around with more **computing** power than the first spaceship that made it to the moon, the **downside**, of course, is that the more interconnected we become, the harder it is to maintain our privacy.

Phone hacking, the act of listening to voicemails, answering phone calls or text messages, has taken centre stage in recent years, not least of which because of the number of high-profile (and alarming) cases of this cybercrime.

As the news emerges, each case has raised deeper concerns about cybersecurity, a topic that many believe to be vital to personal, corporate, and even national security. Recognizing this, policymakers are taking steps to defend these acts. That's a start, but smartphone users should also take action to protect themselves. If you carry a smartphone, here's what you should know.

**How Phone Hacking Works**

In a technologically advanced world, powered by the transfer of information, phone hacking seems an **inevitability**. Whether it's a competitor trying to steal secrets or tabloids looking for stories. But how is it done? The answer may surprise you. In fact, all it takes is a little internet software.

Yup, there's currently lots of software available online that could help virtually anyone get access to call lists, contacts, and text messages. However, most of these tools require direct installation, meaning someone would need access to your phone to download or upload the **spyware.**

Unfortunately, there's also better technology than that. More recently, hackers have found ways to access phones remotely. One of the most common ways this is accomplished is by sending a text message or email with a corrupt link or picture. When the victim clicks on it, the **malware** secretly installs itself onto the phone, where it remains in the background, often undetected. From there, it can send off information including text messages and web history. This kind of software can even allow hackers to hack into a phone camera and control the phone's microphone to listen in on conversations. The good news is that there are many steps that can be taken to prevent phone hacking.

**The Phone You Love**

There's evidence that some phones are more **susceptible** to hacking than others. Unfortunately, exactly which phones fit that description depends on who you ask. Android's "fragmentation" has led many of its critics to believe that it's more susceptible to hacking than its competitors. In addition, the open-source code that gives Android its flexibility also makes security more difficult. This is mainly because hackers have more access to the platform's architecture and can design software specifically customised to extract data. This problem is compounded by the fact that programmers are allowed to openly spread apps without restriction.

Apple's iOS software has a more uncompromising app approval process coupled with more fixed security measures. In theory, that should make iPhones harder to hack. Unfortunately, Apple isn't hack proof either.

The truth is that just about any phone can be hacked, a fact that has raised concerns in the tech community. Some of the responsibility for preventing such attacks lies with smartphone and app developers, but it certainly doesn't hurt for users to take matters into their own hands.

**What To Do To Prevent Your Phone From Being Hacked**

There are many things that can be done to protect your phone from being hacked. Here are a few of the key precautions all smartphone users should take:

**Download Anti-Virus Software**

Anti-virus software can detect and neutralize many forms of spyware that may be hiding in your smartphone. Be sure to download a reliable anti-virus app that can scan your phone for any harmful files that you may or may not have licensed.

**Be Careful About the Apps You Download**

Many of the apps that are widely available to smartphone users come with spyware or **malware**. Make sure that you research each app before you download it to ensure there are no known issues with security.

**Hold Onto Your Phone**

The easiest and most direct type of phone hacking is done to the physical phone itself. For this reason, it's important to be careful about where you leave your phone, and to **ensure** that a password is required to gain access.

**What To Do If Your Phone Has Been Hacked**

Phone hacking is a form of unlawful spying and is considered a federal crime in the United States and many other nations. If you suspect that your phone has been hacked, your first course of action should be to take your smartphone to your service provider. Often, they will be able to verify and even remove spyware and malware. If necessary, they can also assist you in contacting the appropriate law agencies. Of course, you should also change all your passwords and contact any financial or other institutions where you have accounts that you think have been or may be compromised. The best course of action may be to wipe or replace your phone. Of course, it can be a **hassle**, so the best course of action is to avoid phone hacking.

**Phone Hacking in the Future**

Phone hacking is a widespread problem that will only grow with the increasing universality of smartphones. Fortunately, there are many ways to protect your phone, detect when it is being hacked and **remedy** the situation in the case of a phone hack. The best way to handle this issue is to use your smartphone with care. After all, you never know who may be listening in.

**10 Biggest Data Breaches of All Time - And How to Prevent Them**

By **Anas Baig**  
Published: October 10, 2022

Data **breaches** are often the result of simple data management mistakes. You may significantly reduce the risk that your organization will experience a data breach and recover more quickly in the event that it does by putting in place the right data breach prevention measures right away.

**1. Yahoo (2013)**

There's really no other way to start a list of the biggest data breaches ever than with the 2013 Yahoo breach, which affected almost three billion users.

The impact of the breach was a sudden $350 million drop in Yahoo's market value, which happened as they were in the middle of buying Verizon. Although the culprits of the cyberattack were never found, Yahoo said in a statement that it thought "state-sponsored actors" might be to blame.

**2. First American Financial Corporation (2019)**

Nearly a billion records were compromised when the First American Financial Corporation faced a data breach that led to bank account numbers, **mortgage** and tax records, social security numbers, wire transfer receipts and bond transaction receipts being compromised.

What sets this breach apart from the rest on this list is that it wasn't a breach in the traditional sense of the word. Rather than hackers breaking into the databases, the First American Financial Corporation failed to implement a secure authentication protocol which meant no one had to prove their identity to view the documents. Once they accessed the documents, hackers used Advanced Persistent Bots (APBs) to collect, catalog and copy all data they had access to.

This error went unnoticed for years. The New York State Department of Financial Services (NYDFS) claimed the First American Financial Corporation did very little to ensure it had appropriate security measures to protect its critical data.

**3rd Marriott Hotels (2018)**

Marriott is not a typical digital **service provider**, which sets it apart from some of the other names on this list. However, the international hotel chain suffered a breach in 2018 that affected more than 500 million users.

The affected users' contact information, passport numbers, travel history, credit card information, social security details were among the sensitive data that was breached.

**4. MySpace (2016)**

MySpace may not have been as popular as some of the other social networking sites in 2016, but it wasn't any less shocking when the company announced to its users that their old information may be available for sale online -- or, more accurately, that it had been up for sale online for at least three months.

Time Inc., which acquired MySpace, reported a data breach had left 360 million accounts compromised, with their usernames and passwords available to be used to access users' information on other sites. The hackers behind the data breach were thought to be responsible for similar data breaches at Tumblr and LinkedIn.

**5. Adult FriendFinder (2016)**

When Adult FriendFinder suffered a data breach, there was absolute pandemonium all around. This was owed to the nature of the data breach, with information about users' casual hookups and other adult content being made public.

More than 400 users' the names, email addresses, passwords, pictures and other personal details were leaked online and freely available on leaksource.com. The databases compromised had 20 years' worth of information, with the users' credentials also available online. The site's use of **hashing** algorithm -- a fragile protocol by modern standards -- was the primary reason the database was so easily breached.

**6. Twitter (2018)**

How a company the size of Twitter managed to commit such a gaffe will forever remain a mystery. In May 2018, the company sent an email to its 330 million users urging them to change their passwords, since some of their passwords had been stored on its internal computer system in readable text format.

Twitter reassured its users that the glitch had been identified before any data breach, so none of their information had been compromised. However, a 2010 Federal Trade Commission investigation revealed that there had been at least two data breaches at Twitter where users' private data had been compromised due to lapses in Twitter's security protocols**.**

**7. Equifax (2017)**

Compared to some others on this list, the Equifax data breach is fairly mild. However, the fact that the organization had to spend upwards of $700 million in **remedial** measures to help affected users made it a cautionary tale for other organizations.

Approximately 150 million users had their social security numbers, dates of birth, home addresses, driver's license numbers and credit card information stolen. The people responsible for the breach were never identified, even after lengthy congressional **inquiries.**

The inquiries did discover, however, that a **vulnerability** within the Equifax website had been exploited for months by those responsible for the breach. Other inadequate measures, such as the lack of database system segmentation, made the attacks even easier to carry out.

**8. Facebook (2019)**

Facebook was already facing a public relations nightmare in 2019 over its less-than-adequate data protection practices when news of the 2019 breach broke. It was, and remains, the most significant breach in the company's history, affecting up to [540 HYPERLINK "https://techcrunch.com/2019/04/03/facebook-records-exposed-server/"million HYPERLINK "https://techcrunch.com/2019/04/03/facebook-records-exposed-server/" HYPERLINK "https://techcrunch.com/2019/04/03/facebook-records-exposed-server/" HYPERLINK "https://techcrunch.com/2019/04/03/facebook-records-exposed-server/" HYPERLINK "https://techcrunch.com/2019/04/03/facebook-records-exposed-server/"users globally](https://techcrunch.com/2019/04/03/facebook-records-exposed-server/). The perpetrators were never identified or caught, but it did reveal just how **vulnerable** Facebook's databases were.

How did it happen? Facebook had failed to adequately protect its global databases with the appropriate levels of encryption, and these databases were easily searchable online as a result. Users' phone numbers, genders and geolocation in the United Kingdom, United States and Vietnam databases were particularly vulnerable. This is why it proved impossible to identify the perpetrators, since the databases were literally available via a simple Google search with no appropriate security measures to protect them.

**9. eBay (2014)**

The eBay breach came a few months after the Yahoo breach, with similar cases of compromised user data. While the 145 affected comes nowhere near Yahoo's numbers, the impact was not any less severe. Internal investigations revealed three of eBay's employees had been socially engineered, and their compromised credentials were used to gain access to the main eBay database.

The company informed all affected users and advised them to change their passwords, since attackers had accessed encrypted passwords as well. This led to New York's Attorney General calling on eBay to provide free credit monitoring services to users, which the company refused, **citing a lack of financial fraud.**

**10. SolarWinds (2020)**

One of the most recent major data breaches, what makes the SolarWinds data breach so notorious is that there still isn't a reliable number of how many records may have been compromised. However, more than 18,000 organizations and government agencies globally are said to have been affected. The United States Attorney General at the time stated that the attack may have been Russian-backed.

The attackers got insider access to SolarWinds update packages and placed malware into the next scheduled update. These updates contained the necessary e-signatures, so whichever networks accepted the updates were compromised. The hidden malware spread throughout the entire SolarWinds supply chain, with at least 50 United States government agencies facing a "grave impact" since the attackers gained a foothold within their networks.

**Data Breach Prevention: Five Best Practices**

The **aforementioned** list should be reason enough for most organizations to consider a robust data protection and governance framework that can minimize the chance of a data breach occurring.

Here are five some steps most organizations can undertake to do so:

**1. Implement Access Governance**

By far, the most fundamental measure an organization can take to minimize the risk of a data breach is to limit the number of people who have access to the data in the first place -- which is known as **access governance**. There's no shortage of effective solutions that can help organizations address this issue.

**2. Conduct Awareness Trainings**

This may seem rather obvious, but many organizations make the mistake of not appropriately training their employees about just how easily hackers may gain access to the company's databases by exploiting careless employee behavior online.

Regular workshops and training can educate your team on best practices to ensure they follow adequate security protocols online. This could also include anti-phishing training on adequately securing their footprint online via cybersecurity tool such as anti-virus software.

**3. Update Regularly**

Yet another example of a relatively minor mistake that can lead to significant damage: Far too often, hackers **exploit glitches** in the software.

If an organization does not update its software regularly, the glitch will likely be present for that entire duration and can be exploited more easily.

**4. Have a Proactive Response Plan**

Often, organizations are too rattled and disorganized if they do find themselves victims of a data breach. It's worth mentioning that, if proper measures are taken in the immediate aftermath of a data breach, the impact of the breach can be drastically reduced.

You should have protocols in place that can give real-time insights into exactly what data was compromised, how the damage can be limited and the remedial measures most necessary.

**5. Encrypt, Encrypt, Encrypt**

Last, but probably the most important, is to know exactly how to leverage encryption to your benefit. Organizations that have an old-fashioned approach to encryption fail to maximize the security encryption has to offer.

With lattice-based encryption and quantum computing now gathering steam, organisations can afford to ensure the best possible protection for all their data. Doing so guarantees that, if everything else fails, your data is so well-protected that hackers gain nothing by breaking into the company's internal database.

**Conclusion**

Data breaches can happen to anyone -- even the largest, most well-established organizations. And often, they're the result of simple, easily solvable data management mistakes. By implementing proper data breach prevention practices beforehand, you can drastically reduce the likelihood of your organization suffering a data breach and recover more efficiently in the worst-case scenario.

**How Automated Threat Recognition Technology Enhances Airport Security**

By **Kuntal Chakraborty**

Automated threat recognition technology at airports is being developed to keep air travel safe.

With airports and airlines struggling to keep up with passenger demand and staffing issues, air travel is challenging in a thousand different ways. What hasn't changed, in this sea of change, is the importance of safety. The technology used for safety measures and screening, however, is undergoing some exciting developments.

AI has invented a new software that can detect threats and enhance airport security to assure safer travel. This article will discuss how automated threat detection technologies increase security at airports.

**What Is Automated Threat Recognition?**

Automated Threat Recognition (ATR) software examines physical items or human body scan data to detect areas where contraband can be kept hidden. These identified sections are flagged on a standardized display to inform the security officer which areas to perform a manual search on.

Scanners perform automated threat recognition on images to detect threat objects. Enhanced automated threat recognition will improve the detection of threatening items. Advanced [automated target recognition](https://www.techopedia.com/definition/30414/machine-vision-system-mvs) algorithms will help enhanced 3D Computed Tomography (CT) Scanners-CT-based object detection equipment-by enhancing object recognition techniques, similar to CT scans that are performed at the hospital on brains!

**The Challenges Of Airport Authorities and Government**

Created in the wake of the 9/11 terrorist attack in the US, the Transportation Security Administration (TSA) is tasked with protecting United States air travel. They hire human inspectors to check passengers and baggage for **prohibited** items and threats using scanners and x-ray images. This task sometimes becomes difficult, particularly when you consider that often the machines used don't communicate with each other. There is an **acute** need for improvement.

The Open Threat Assessment Platform (OTAP) project is working to change stats like this. Researchers from Stratovan and Sandia Nationwide Laboratories are taking an important role in airport safety innovation. They are working from the position that some existing technology and processes are too rigid and needlessly time-consuming. For instance, having everyone enforcing the current restrictions on aerosols, liquids and gels could possibly be approached differently.

Travelers who are now used to today's standards may be surprised to know that prior to 9/11, things were very different for those departing US airports:

* Blades up to 4 inches were permitted on the plane.
* Baseball bats, box cutters, darts, and scissors were also allowed on the plane.
* Family members were able to go through security to the departing gate to say goodbye.
* Passengers could keep shoes on when going through security.
* Passengers could carry liquids onto the plane.
* The only security screening was a metal detector.
* No ID was required.
* Passengers would only need to arrive 30 minutes before their flight to ensure they would make their flight.

Over the last two decades, airports across many countries have worked on their security enhancement to prevent **emerging threats.** They are trying hard to make the journey from entrance to exit gate as seamless as possible.

For many governments and aviation centres, the improvement of artificial intelligence is the best solution. The UK Government has already invested £1.8m into the development of new AI security systems, a **full-scale roll out** of new biometric services**,** and are working to reduce wait times across some of their busiest airports.

The US Transportation Security Administration has implemented new CT scanners, which utilize AI to help target threats, at Los Angeles International Airport, John F. Kennedy and Phoenix airports.

**AI Software for Security Systems**

AI is implemented across the entire aviation spectrum, from self-service check-in robots to facial recognition checks at customs. On the other side, recent research applying deep learning techniques to computer-aided security screening to assist operators showed encouraging results.

AI systems work on various datasets. For airport security, technologists use machine learning to analyse data and identify threats faster than humans. Objects that previously needed to be scanned separately, can be kept in passenger luggage as they pass through security checkpoints.

The OTAP project described above was developed with many aviation security industry partners including algorithm developers, X-ray vendors and software specialists to build the Open Platform Software Library (OPSL).

Similarly, Pacific Northwest National Laboratory developed a High-Definition Passenger Imaging System, which can scan a body. In 2017, Sandia joined forces with PNNL to add the scanner with OPSL to make an advanced full-body machine that can more accurately detect threats.

The team is now using automated threat recognition software sensors-CT and AIT systems-by testing with bags, toiletries, laptops, and simulated explosives, to show the device's **accuracy**.

**AI-Powered Baggage Screening**

Airport Authority Of India (AAI) has chosen eight airports to test the capabilities of Artificial Intelligence in baggage screening. Pune airport is one of them, which implemented the '"Baggage AI" system. The AI-powered device strengthens the security efforts at the airport.

Baggage AI is an artificial intelligence-based model which is the threat detection system for security x-ray machines. This AI software can automatically identify various objects and other threats from the x-ray images created during the screening of baggage and alert operatives.

**Use Of Biometrics In Airport Security**

One remarkable invention in AI is biometrics. Major airports have decided to use biometric ID management over the next couple of years. The primary purpose of biometrics is facial recognition, which is already operational to scan passengers as they pass through customs at a number of major airports. Passengers can use facial recognition scanners at **self-service kiosks**, TSA checkpoints, or boarding gates. Fingerprinting, facial recognition, and retinal scans can become essential verification methods for security screening at airports.

**Conclusion**

Past failures and present-day threats have created an urgent need for these advanced AI-based technologies in airport security. Technology that reduces passenger friction during the hustle and bustle of travel, not having to take belts off, and keeping your shoes on has got to be a positive step for air travelers. AI not only can identify known threats but also detects unknown threats. AI is an integral part of cybersecurity, including its machine learning model. As automated threat recognition systems through AI advance over time, terrorist attacks could be predicted and controlled. More safety in the airports assures a peaceful journey for passengers.