



R&D Cell, CTCT & IT

NEWS LETTER



January, 2020



CTCT & IT, Ranchi, Jharkhand



Shri Amit Taneja, DIGP
Patron

Shri Rajesh Sahay, Comdt.
Chief Editor

Shri Sanjay Belwal, DC.
Editor & Publisher

Index

Sl	Topic	Author	Page No
1.	Privacy On Mobile Devices	SI/T Najas Ali A.K.	3
2.	Graphene Technology	ASI/T C Vijay Kumar	5
3.	Green Information Technology	HC/RO Dhananjay Kumar	7
4.	BIOS Vs UEFI Of Computer System	HC/RO Chandan Kumar	8
5.	SIM Card	R & D Team	10
6.	Quiz	R & D Team	12
7.	Technical Terms	R & D Team	14
8.	Answers To Quiz	R & D Team	15

“Turn your wounds into wisdom”

PRIVACY ON MOBILE DEVICES

SI/T Najas Ali A.K.

These days, smartphones are a one-stop payment, personal health, work, gaming, productivity, texting, tweeting, Facebook-checking machine. We use them to do just about everything, from mobile banking to navigating new places, to emailing out last minute notes on a project.

But whether it's hacked browsers, petty thieves at the coffee shop, or your own tendency to lose electronics in cabs, using your smartphone as a centralized source for all of your information comes with big risks, and the more you've connected and stored, the more you stand to lose. In fact, in the last year alone, at least 7.1 million phones were lost or stolen.

It's no wonder, then, that so many individuals and businesses are starting to take mobile security seriously. Let's take a look at few steps you can take to keep your phone—and its wealth of personal data—secure.



1. Use a Passcode

This may sound obvious, but according to a Consumer Reports survey, 64% of us don't use our passcodes. (For the record, using the factory set passcode totally doesn't count.) Quite frankly, not using a passcode is a horrible idea. You're essentially handing over all of your personal information to anyone who swipes your phone.

When you set up your passcode, use the same security measures you would on any other device, such as not using your birthday or social security number for your passcode, and definitely not "1234." Never share your passcode with anyone, even if they ask nicely or give you sad, puppy eyes. Don't reuse passwords from other sites or devices.

2. Be Selective with Your Apps

That new app might look great, but with so many unknown third-party providers out there, it can be difficult to know how private and secure it may be. For that reason, it's best to go through a trusted app store like iTunes, Android Market or Amazon, and to thoroughly check reviews before downloading any app and entering your personal information.

3. Don't Click on Suspicious Links

Maybe it's those tiny, almost indecipherable screens, maybe it's a false sense of security, but for some reason, people are three times more likely to click on suspicious links on their cell phone than on a PC. Our best advice for that? Don't do it. Look more carefully at the URL, especially if they're asking you to enter personal information. Most banks have a page explaining what they will and will not ask for. Do your research before divulging your personal details.

4. Enable Remote Wiping

Should your phone ever be lost or stolen, it would be great to erase your important data from afar. You can do this through remote wiping, and it's relatively easy to do on most devices. An iPhone, for example, simply requires you to do enable "Find My Phone" on the device and to sign up for an iCloud account, which will be your command central when it's time to wipe.

There are some concerns about corporations using location tracking software like this to infringe upon personal privacy rights. Look up the company's policy, and make sure it's something you're comfortable with, before getting it all set up.

5. Keep Software Up to Date

Software updates often patch security and privacy holes users have found as they've tested the software out in the real world. Keeping your software up to date will mean you'll have the very

latest solutions. That said, sometimes it makes sense to wait a week, or two, before installing the latest versions to see if there are any problems with rollouts.

6. Use Security Applications

Both Spyware and Malware are becoming an increasingly formidable problem for mobile phone users. They track your whereabouts, send out your personal information, and slow down your phone. It can be difficult to avoid downloading these, and users often don't know they're running. To combat this, install security software, just like you might have on your computer, to protect your privacy against any unbeknownst mischief. Make sure that you keep this software up to date.

7. Stay Off of Open Wi-Fi Networks

Since smartphones are now acting like mini-PCs, avoid unknown open Wi-Fi networks, just like you would on your PC. As you type, malicious hotspots can transmit your credit card information and passwords without you even knowing it.

8. Write Down Your IMEI

Every phone has a fifteen digits serial number called an IMEI (International Mobile Equipment Identity), which can come in handy if your phone is ever lost or stolen. You'll find it behind your phone's battery or in the settings. It's well worth writing down, as it can speed the process of getting the phone back to you.

9. Back Up Your Phone Regularly

Backing up your phone means you'll always have access to all of your photos, music, apps and whatever else. This is of course important in case your phone gets lost or stolen, but it can also come in handy when you're doing an OS update and experience a loss of data (it happens). Make sure to back up at least once a day for the best results, or consider using automatic syncing with a cloud program.

10. Guard the Data on Your Sim Card

If you decide to sell your cell phone, there are a number of things you should do before shipping it off to a stranger. One of the most important is to remove both your SIM and your SD card, both of which contain a wealth of data. Do this when sending your phone in for repairs, as well, particularly if you don't know your repair shop well.

The Takeaway

There are many security risks for smartphone users today, and these risks will continue to grow along with the devices' popularity. Protect your phone, your data, and yourself by implementing just a few simple measures. Good luck, and stay safe.

GRAPHENE TECHNOLOGY

ASI/T C Vijay Kumar

Graphene is the name for a honeycomb sheet of carbon atoms. It is the building block for other graphitic materials (since a typical carbon atom has a diameter of about 0.33 nanometres, there are about 3 million layers of graphene in 1 mm of graphite). Harder than diamond yet more elastic than rubber; tougher than steel yet lighter than aluminium. Graphene is the strongest known material. To put this in perspective: if a sheet of cling film (like kitchen wrap film) had the same strength as a pristine monolayer of graphene, it would require the force exerted by a mass of 2000 kg, or a large car, to puncture it with a pencil. Graphene possesses other amazing characteristics: Its high electron mobility is 100x faster than silicon; it conducts heat 2x better than diamond; its electrical conductivity is 13x better than copper; it absorbs only 2.3% of reflecting light; it is impervious so that even the smallest atom (helium) can't pass through a defect-free monolayer graphene sheet; and its high surface area of 2630 square meters per gram means that with less than 3 grams you could cover an entire soccer field (well, practically speaking you would need 6 grams, since 2630 m²/g is the surface area for both sides of a graphene sheet). Graphene is the basic building block for other graphitic materials; it also represents a conceptually new class of materials that are only one atom thick, so-called two-dimensional (2D) materials (they are called 2D because they extend in only two dimensions: length and width; as the material is only one atom thick, the third dimension, height, is considered to be zero). Graphene is also very attractive for the fabrication of mixed-dimensional van der Waals heterostructures that could be carried out through hybridizing graphene with 0D quantum dots or nanoparticles, 1D nanostructures such as nanowires or carbon nanotubes, or 3D bulk materials. The most famous molecule in the tech industry is coming to life it's strong, it's flexible, and it's now been here for a while. It spent a long time being refined and developed in the labs, but graphene has been on the market for a couple of years now and it's having an impact. The first wave of graphene-based products are being used in the world of smartphones, wearables, batteries, virtual reality, sports equipment, super-capacitors and supercars and that's just the beginning. Graphene is a material that some believe has been coerced from abandoned space ships, left on Earth by extra-terrestrials years ago. While that's a little unlikely, the power of this super-thin, strong, conductive and all-round amazing material is deserving of such a conspiracy. It has been over 60 years coming as scientists and manufacturers alike have struggled to harness the power of this awesome material, but it's closing in on revolutionizing so many things we're using day to day.

more ways that graphene is about to change your life.

Graphene nano-electronics

Ultra-thin and 2D, graphene conducts electrical current like nothing else, which in theory should mean much faster and more energy-efficient forms of electronics. What has been holding it back is the band-gap problem; how to engineer a graphene transistor that reliably switches on and off.



Fitness Patch

Since it is flexible and extremely sensitive to changes in heat and light, graphene has a big future in wearable devices. This 'transdermal fitness patch' from the ICFO in Barcelona does everything your Fitbit can do, and more, but in the form of a stick-on patch. It measures heart rate, hydration and breathing rate with improved accuracy and less power consumption than current fitness bands, and conforms to any surface.



This is sadly still just a prototype right now, but the ICFO believes that it could easily connect to your smartphone and give you alerts when you're a little bit dehydrated because we're so busy looking at our phones that we've forgotten to note when we're thirsty.

Graphene brain-computer interfaces

Flexible graphene circuits can be laid over the human brain. Image credit: Valdek Laur (EU2017EE) / Graphene Flagship Flexible graphene circuits can be laid over the human brain. Image credit: Valdek Laur (EU2017EE) / Graphene Flagship Graphene's flexibility means it can be used in brain implants that record and stimulate brain signals on the surface of the brain. Graphene is enabling a new generation of less-invasive neural implants, It can be easily integrated into flexible substrates, it has a very high signal-to-noise ratio so retains a very high quality electrical signal, and it also minimizes the use of cables. Garrido's work at the ICN2 Speech Centre Stimulation and BrainCom is focusing on providing a communication path to patients with severe speech disabilities (such as strokes and motor neuron disease) by mapping the region of the brain correlated to pronouncing speech.



Graphene may not yet be commercially available but in the coming years is almost certainly going to be applied in many different fields. Just one atom thick and less than fifty atoms (a few nano meters) wide, the tiny transistor made from graphene pave the way for a new breed of computer chips smaller and faster than those based on silicon.

GREEN INFORMATION TECHNOLOGY

HC/RO Dhananjay Kumar

In this modern world everything goes through technology, and because of this our environment is not in safe condition. Green IT is not only a new trend; it is a technology of itself. The move to become more environmentally friendly is more than just a means to a better image. So it's time to change our need according to our environment.

- ❖ Green IT, also known as green computing, means energy-saving and waste-reducing practices should be adopted in information technology field. As the cost of energy is going up, and the disposal of electronic waste is becoming a major issue, IT departments must learn about and implement green IT practices.
- ❖ Green IT (green information technology) is the practice of environmentally sustainable computing.
- ❖ Green IT aims to minimize the negative impact of IT operations on the environment by designing, manufacturing, operating and disposing of computers and computer-related products in an environmentally-friendly manner. The motives behind green IT practices include reducing the use of hazardous materials, maximizing energy efficiency during the product's lifetime and promoting the biodegradability of unused and outdated products.
- ❖ If we all go through green IT so many benefits, we can see
 - reduced environmental impact (less e-waste, fewer virgin resources needed for manufacturing new devices)
 - lower energy costs.
 - longer lasting computing devices.
 - reduced health risk for computer workers and recyclers.

BIOS Vs UEFI OF COMPUTER SYSTEM

HC/RO Chandan Kumar

INTRODUCTION:- Unified Extensible Firmware Interface (UEFI) is a specification for a software program that connects a computer's firmware to its operating system (OS). UEFI is expected to eventually replace BIOS. Like BIOS, UEFI is installed at the time of manufacturing and is the first program that runs when a computer is turned on. The older BIOS (Basic Input/Output System) and its modern replacement UEFI (Unified Extensible Firmware Interface) can both be seen as the "firmware" of your computer. Most UEFI systems also support CSM (Compatibility Support Module) booting, which emulates a Legacy BIOS interface.



Advantages:-

The interface defined by the EFI specification includes data tables that contain platform information, and boot and runtime services that are available to the OS loader and OS. UEFI firmware provides several technical advantages over a traditional BIOS system.

- Ability to use large disks partitions (over 2 TB) with a GUID Partition Table (GPT)
- CPU-independent architecture.
- CPU-independent drivers.
- Flexible pre-OS environment, including network capability.
- Modular design.
- Backward and forward compatibility.

Why the BIOS Is Outdated:-

The BIOS has been around for a long time, and hasn't evolved much. Even MS-DOS PCs released in the 1980s had a BIOS. Of course, the BIOS has evolved and improved over time. Some extensions were developed, including ACPI, the Advanced Configuration and Power Interface. This allows the BIOS to more easily configure devices and perform advanced power management functions, like sleep. But the BIOS hasn't advanced and improved nearly as much as other PC technology has since the days of MS-DOS.

The traditional BIOS still has serious limitations. It can only boot from drives of 2.1 TB or less. 3 TB drives are now common, and a computer with a BIOS can't boot from them. That limitation is due to the way the BIOS's Master Boot Record system works. The BIOS must run in 16-bit processor mode, and only has 1 MB of space to execute in. It has trouble initializing multiple hardware devices at once, which leads to a slower boot process when initializing all the hardware interfaces and devices on a modern PC.

The BIOS has needed replacement for a long time. Intel started work on the Extensible Firmware Interface (EFI) specification back in 1998. Apple chose EFI when it switched to the Intel architecture on its Macs in 2006, but other PC manufacturers didn't follow.

How to Access UEFI Settings on Modern PCs:-

If you're a normal PC user, switching to a computer with UEFI won't be a noticeable change. Your new computer will boot up and shut down faster than it would have with a BIOS, and you can use drives of 2.2 TB or more in size.

While UEFI is a big upgrade, it's largely in the background. Most PC users will never notice or need to care that their new PCs use UEFI instead of a traditional BIOS. They'll just work better and support more modern hardware and features.

SIM Card

R&D Team

SIM card is a smart card used to make communication between the users. It is a convenient memory card utilized basically as a part of phones that work universally for communication. The SIM cards hold the individual information of the record holder including his or her telephone number, location book, instant messages and its related information. A SIM circuit is installed into a removable plastic card. This plastic card is known as a "**SIM card**" and can be exchanged between distinctive mobile gadgets. The advancement of physically mini mobile gadgets causes the improvement of mini SIM cards where the amount of card encompassing the integrated circuit is decreased.

Internationally each SIM cards are identified by ICC-ID, which means Integrated Circuit Card ID. During personalization process this ICC-ID is stored or printed on the SIM cards. This ID contains 18-digit numbers along with single check digit for error detection. This digit was calculated using Luhn Algorithm. It helps to detect mistyped digit or error in input digits. These 18 digits are further classified into three types. First one is a group of 7 digits which contains major industry identifier, Country code, Issuer Identifier number. Rest of number represents Individual account identification number, then the last digit is checksum digit. Let us consider 81 91 23 1311 00 143547 be the 18-digit ID. From this number,

First two digits (81) – represents major industry identifier

Next two digits (91) - Country code

Next two digits (23) – Issuer identifier number

Next four digits (1311) – month and year of manufacturing

Next two digits (00) – Switch configuration code

Next six digits (143547) – SIM number

Security

A SIM card offers security for both the client's information and his or her calls. The cards can be bolted implying that just somebody who has the right individual identification number (PIN) can utilize the card. On the off chance that the telephone is stolen, the criminal can't utilize a bolted SIM or get any information off of it without the PIN.

Further, the card has a mystery confirmation code and an encryption scratch that ensures the telephone's transmissions. Despite the fact that it is conceivable to "clone" a cell on the Global System for Mobile Communications network and in this way take services. It's substantially more troublesome than it is to clone a telephone on the contending Code Division Multiple Access network. In view of the way the encryption information is transmitted to the bearer. It's typically important to have physical access to the SIM card with a specific end goal to duplicate it. For any investigation, the investigator can collect some details like incoming/outgoing call details, SIM contact, SMS details etc. from SIM card. Some soft wares are also available now for recovering information from SIM cards.

Types of SIM cards

There are a couple of diverse SIM cards we have accessible. The working of all SIMs is same but one difference that they come in different shapes. Your phone's intended to take one specific shape SIM, so verify you've pick up the privilege one for your cell phone or Smartphone. Here are a few illustrations:

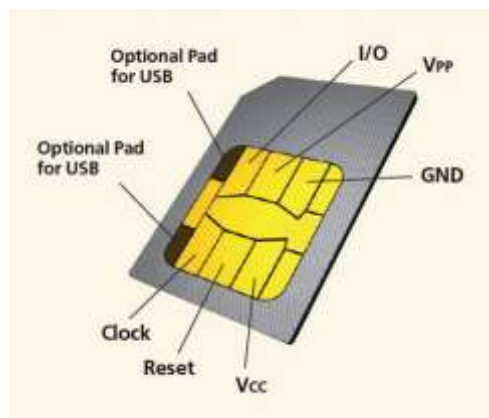


Standard SIM card

It is the largest in size among all the available SIM cards. Standard SIM card are widely used in these days in the cell phones and tablets. The size of standard SIM card is **2.5** centimetres long and **1.5** centimetres broad.

Micro SIM cards

The micro-SIM was intended for retrogressive similarity. The real issue for regressive similarity was the connection range of the memory. Holding the parallel connection zone permits the micro-SIM to be perfect with the earlier, bigger SIM peruses through the utilization of plastic set pattern encompasses.



Nano SIM cards

The 0.67 mm thickness of the NANO SIM is around 12% not exactly the 0.76 mm of its forerunner. 4ff can be put into connectors for utilization with gadgets taking 2ff or 3ff Sims; numerous telephone organizations however don't suggest utilizing these adapters. The iPhone 5 discharged in September 2012, was the first gadget to utilize a Nano-SIM card emulated by different handsets including the Nexus. It is newly come in the market used in the smartphones.

Other than the conspicuous focal point of being littler there isn't essentially preference to utilizing a littler SIM card.

Working of SIM card

The stored datas in SIM cards are ICC ID, IMSI (International Mobile Subscriber Identity), Information about the network, Security Authentication Information, PIN (Personal Identification Number), PUK Code, Users information and GSM/CDMS identity. Each SIM card has an internal data storage system. If you start up the one more of a cell phone that is outfitted with an SIM card, you will see the card fold into the cell phone. Typically, the card is fold behind the battery. SIM cards are furthermore incredible on the grounds that they can be utilized with any handset that supports them. For instance, whenever your cell phone failure and you are not able to do calls from it, yet at the same time have a dynamic SIM card, you are in luckiness. Simply get your SIM card from the cell phone and fitting it into another cell phone and start communication with a new phone using same SIM card. SIM cards are encoded with data regarding the transporter that you are utilizing and additionally data like your location book. And hold data similar this on an SIM card will permit you to make a quick and straightforward switch over to an alternate telephone on the same transporter, or to switch transporters totally.

On a few networks the cellular telephone is bolted to its SIM card for example, on the GSM networks in the USA. This has a tendency to happen just in countries where cell telephones are intensely sponsored, however that being said not all countries and not all operators. For example, and in the UK regularly most telephones with appropriations are not SIM bolted. In countries where the telephones are not sponsored, for example, Italy and Belgium, all telephones are opened. Where the telephone is not bolted to its SIM card, the clients can undoubtedly switch networks by essentially supplanting the SIM card of one network with that of an alternate while utilizing one and only telephone. This is normal for instance among youthful clients who may need to improve their telecoms activity by distinctive levies to diverse companions on distinctive networks. It is known as the "**SIM card switch**"

Technical Quiz

R&D Team

1. The Government of India has launched the “Central Equipment Identify Register” portal to trace what?
 - a) Lost Mobiles
 - b) Lost Vehicles
 - c) Missing Children
 - d) Criminals
2. The Road Transport Corporation of which state has launched a dedicated women helpline, 'Damini' ?
 - a) Madhya Pradesh
 - b) Uttar Pradesh
 - c) Gujarat
 - d) Rajasthan
3. Railway Protection Force (RPF) has been renamed as _____ ?
 - a) Indian Railway Protection Force
 - b) Indian Railway Protection Force Service
 - c) Indian Railway Protection Task Force
 - d) Indian Railway Protection Group
4. Which state has decided to celebrate the first day of the month as 'No Vehicle Day' from 2020?
 - a) Madhya Pradesh
 - b) Gujarat
 - c) Jharkhand
 - d) Rajasthan
5. RBI has launched which app to help visually challenged identify currency notes?
 - a) BANI
 - b) MANI
 - c) VANI
 - d) NANI

6. Which state has launched the “Pauti” App to facilitate online payment of land revenue?
- a) Andhra Pradesh
 - b) Rajasthan
 - c) Karnataka
 - d) Odisha
7. ISRO has signed a pact with Indian Institute of Astrophysics to establish an optical telescope under which project?
- a) NETRA
 - b) DHRUV
 - c) TANISHQ
 - d) TOPCHI
8. AI powered National Stock Exchange Knowledge Hub was recently inaugurated in which city?
- a) Jaipur
 - b) Mumbai
 - c) New Delhi
 - d) Bengaluru
9. Who has been named as the Telecom Person of the Year for 2019?
- a) Sunil Kumar Gupta
 - b) Abhay Karandikar
 - c) Ram Sewak Sharma
 - d) Shailendra Kumar Mishra
10. Which state has decided to ban all types of online lottery schemes in the state?
- a) Haryana
 - b) Madhya Pradesh
 - c) Punjab
 - d) Odisha

Technical Terms

R&D Team

Algorithms:

A set of rules or instructions given to an AI, neural network, or other machines to help it learn on its own; classification, clustering, recommendation, and regression are four of the most popular types.

Artificial neural network (ANN):

A learning model created to act like a human brain that solves tasks that are too difficult for traditional computer systems to solve.

Cognitive computing:

A computerized model that mimics the way the human brain thinks. It involves self-learning through the use of data mining, natural language processing, and pattern recognition.

Decision tree:

A tree and branch-based model used to map decisions and their possible consequences, similar to a flow chart.

Deep learning:

The ability for machines to autonomously mimic human thought patterns through artificial neural networks composed of cascading layers of information.

Knowledge engineering:

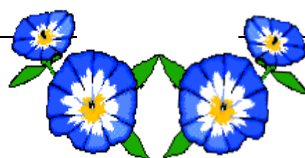
Focuses on building knowledge-based systems, including all of the scientific, technical, and social aspects of it.

Logic programming:

A type of programming paradigm in which computation is carried out based on the knowledge repository of facts and rules; LISP and Prolog are two logic programming languages used for AI programming.

Acknowledgement

We are highly thankful for reading out this compilation and hope it will be useful for you in our day to day professional and personal life. We would like to hear your interest areas, suggestions from you to make this newsletter more informative and interesting. Your views will definitely help us to create this newsletter as an effective medium to reach you with latest development in the fields of communication and technology.



R&D Team

CTC T&IT CRPF, Ranchi, Jharkhand

✉ ctcit@crpf.gov.in

Answers to the Quiz

1	2	3	4	5	6	7	8	9	10
A	B	B	D	B	D	A	C	C	C