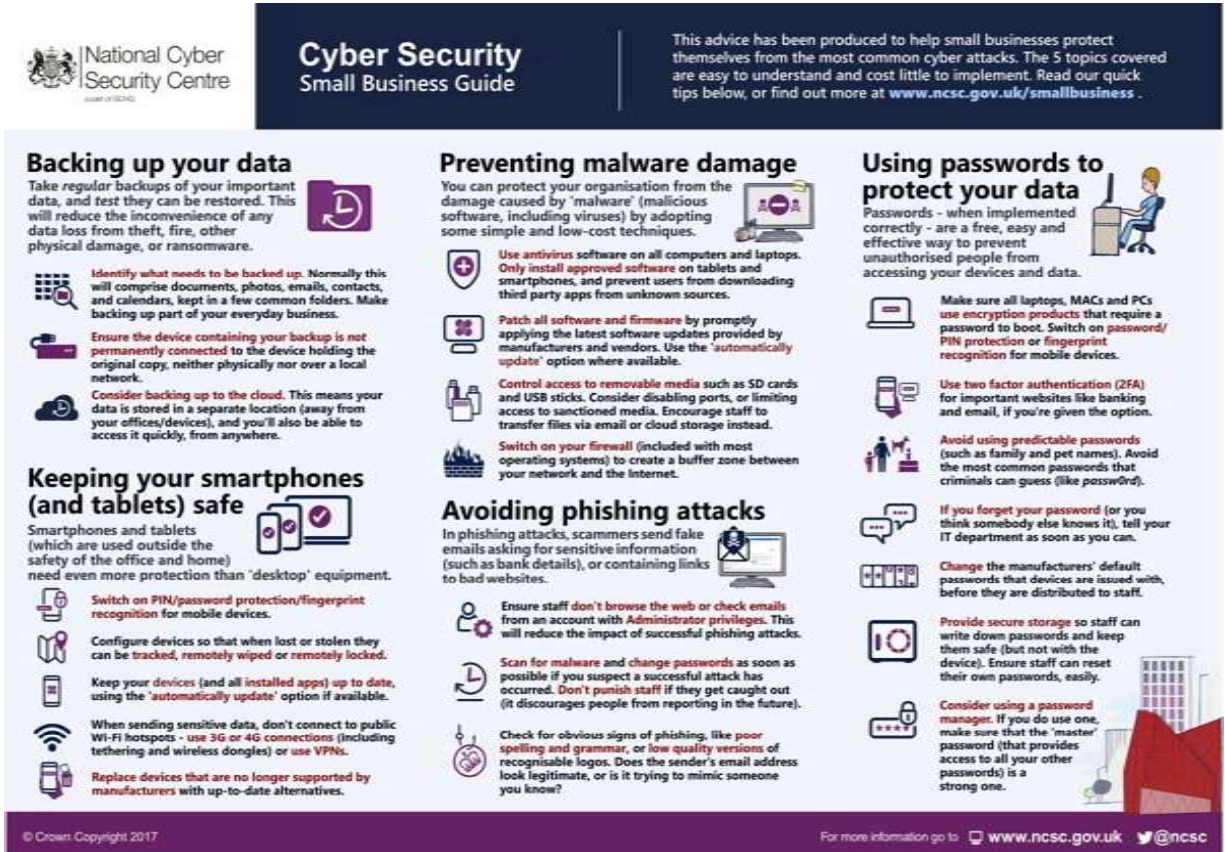


# DID YOU KNOW (An Initiative by Scholastic Seed Inc.)

Did You Know (DYN): DYN aims to achieve and fulfill the goals in readers' mind. The purpose is very clear and understandable that it showcases new and improved content, illustrating readers continuous improvement and expansion of cyber thoughts. It also highlights the variety of information on cyber and thereby provide an insight into the range of material that magazine covers. it includes the facts about a range of topics which may not essentially recognized in the main article disclosure.



**National Cyber Security Centre**  
Small Business Guide

This advice has been produced to help small businesses protect themselves from the most common cyber attacks. The 5 topics covered are easy to understand and cost little to implement. Read our quick tips below, or find out more at [www.ncsc.gov.uk/smallbusiness](http://www.ncsc.gov.uk/smallbusiness).

### Backing up your data

Take regular backups of your important data, and test they can be restored. This will reduce the inconvenience of any data loss from theft, fire, other physical damage, or ransomware.

- Identify what needs to be backed up. Normally this will comprise documents, photos, emails, contacts, and calendars, kept in a few common folders. Make backing up part of your everyday business.
- Ensure the device containing your backup is not permanently connected to the device holding the original copy, neither physically nor over a local network.
- Consider backing up to the cloud. This means your data is stored in a separate location (away from your offices/devices), and you'll also be able to access it quickly, from anywhere.

### Preventing malware damage

You can protect your organisation from the damage caused by 'malware' (malicious software, including viruses) by adopting some simple and low-cost techniques.

- Use antivirus software on all computers and laptops. Only install approved software on tablets and smartphones, and prevent users from downloading third party apps from unknown sources.
- Patch all software and firmware by promptly applying the latest software updates provided by manufacturers and vendors. Use the 'automatically update' option where available.
- Control access to removable media such as SD cards and USB sticks. Consider disabling ports, or limiting access to sanctioned media. Encourage staff to transfer files via email or cloud storage instead.
- Switch on your firewall (included with most operating systems) to create a buffer zone between your network and the Internet.

### Using passwords to protect your data

Passwords - when implemented correctly - are a free, easy and effective way to prevent unauthorised people from accessing your devices and data.

- Make sure all laptops, MACs and PCs use encryption products that require a password to boot. Switch on password/PIN protection or fingerprint recognition for mobile devices.
- Use two factor authentication (2FA) for important websites like banking and email, if you're given the option.
- Avoid using predictable passwords (such as family and pet names). Avoid the most common passwords that criminals can guess (like password).
- If you forget your password (or you think somebody else knows it), tell your IT department as soon as you can.
- Change the manufacturers' default passwords that devices are issued with, before they are distributed to staff.
- Provide secure storage so staff can write down passwords and keep them safe (but not with the device). Ensure staff can reset their own passwords, easily.
- Consider using a password manager. If you do use one, make sure that the 'master' password (that provides access to all your other passwords) is a strong one.

### Keeping your smartphones (and tablets) safe

Smartphones and tablets (which are used outside the safety of the office and home) need even more protection than 'desktop' equipment.

- Switch on PIN/password protection/fingerprint recognition for mobile devices.
- Configure devices so that when lost or stolen they can be tracked, remotely wiped or remotely locked.
- Keep your devices (and all installed apps) up to date, using the 'automatically update' option if available.
- When sending sensitive data, don't connect to public Wi-Fi hotspots - use 3G or 4G connections (including tethering and wireless dongles) or use VPNs.
- Replace devices that are no longer supported by manufacturers with up-to-date alternatives.

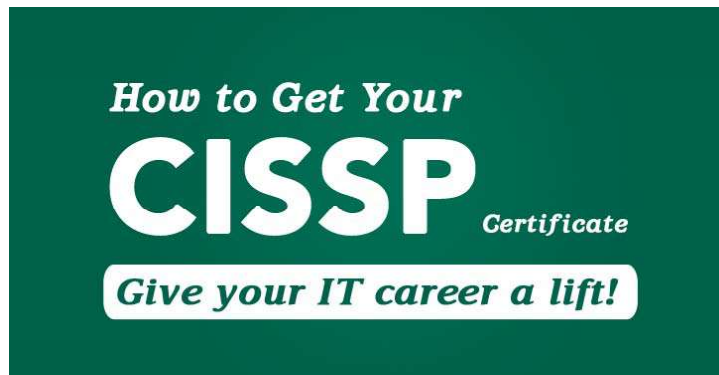
### Avoiding phishing attacks

In phishing attacks, scammers send fake emails asking for sensitive information (such as bank details), or containing links to bad websites.

- Ensure staff don't browse the web or check emails from an account with Administrator privileges. This will reduce the impact of successful phishing attacks.
- Scan for malware and change passwords as soon as possible if you suspect a successful attack has occurred. Don't punish staff if they get caught out (it discourages people from reporting in the future).
- Check for obvious signs of phishing, like poor spelling and grammar, or low quality versions of recognisable logos. Does the sender's email address look legitimate, or is it trying to mimic someone you know?

## What is CISSP?

Certified Information Systems Security Professional (CISSP) is a globally recognized certification in the field of information security, which is governed by the International Information Systems Security Certification Consortium, commonly known as (ISC) <sup>2</sup>.



**How to Get Your**  
**CISSP** Certificate  
**Give your IT career a lift!**

CISSP has become a standard of achievement that is acknowledged worldwide. The exam is highly challenging, and requires a broad level of knowledge. Moreover, achieving it requires help, irrespective of your experience level.



## About Automotive Grade Linux (AGL)

Automotive Grade Linux (AGL) is a collaborative open source project that is bringing together automakers, suppliers and technology companies to build a Linux-based, open software platform for automotive applications that can serve as the de facto industry standard. Adopting a shared platform across the industry reduces fragmentation and allows automakers and suppliers to reuse the same code base, leading to rapid innovation and faster time-to-market for new products.

As a "code first" organization, AGL's goals are to:

- Build a single platform for the entire industry
- Develop 70-80% of the starting point for a production project
- Reduce fragmentation by combining the best of open source
- Develop an ecosystem of developers, suppliers, expertise all using a single platform



Although initially focused on infotainment, AGL is the only organization planning to address all software in the vehicle- infotainment, instrument cluster, head-up-display (HUD), telematics/ connected car, advanced driver assistance systems (ADAS), functional safety and autonomous driving.

Automotive Grade Linux is a Project at [The Linux Foundation](https://www.linuxfoundation.org/).

Source: <https://www.automotivelinux.org>



Source: <https://www2.deloitte.com/us/en/insights/focus/tech-trends/2020/ethical-technology-and-brand-trust.html>





Scholastic Seed Inc.

Indian Cyber Industry Flag March (ICIFM) is a new initiative by Scholastic Seed Inc. and Cybernomics together to throw a light on these indigeneous conglomerate houses which have crossed the Indian boundaries and put indian flags up outside by their innovative thought and creation. The Intention is to show a glimpse of their initiative vis-a-vis Cyber security, online threats and greater significance in today's digital changing landscape and how these indigenous firm are sustaining due to threat in cybercrime activities in the global digital era.

### Infosys opens new cyber defence centre in Romania

Infosys announced the launch of its state-of-the-art Cyber Defence Center in Bucharest, Romania. The Defence Center is an expansion of services delivered through the Infosys Digital Innovation Center which opened in Bucharest earlier this year.



Source: Infosys

The Defence Center will provide end-to-end, real-time, 24/7 cyber security monitoring and protection services to support European and global businesses on their digital transformation journey. These services, including security monitoring, management and remediation, threat hunting, security analytics, incident discovery and response, will be delivered by certified and highly skilled cyber security professionals. The services offered comply with country-specific regulatory requirements.



Source: <https://www.romania-insider.com/infosys-cybersecurity-center-bucharest>

IT services and consultancy provider Infosys, one of India's largest outsourcing companies, announced the opening of a cyber-security center in Bucharest, thus extending the range of services provided through by its digital innovation center inaugurated in Romania's capital city in March this year.

The Cyber Security Center will provide full 24/7 real-time monitoring and cyber-protection services to support European and global companies in their digital transformation.

In 2018, the local subsidiary of Infosys had 65 employees and registered revenues of RON 20.03 million (EUR 4.3 mln), twice as much as in the previous year, and a net profit of about RON 1 mln (EUR 220,000), not much changed compared to the year before.

### The next

We bring you powerful advantages to navigate your digital transformation



Source: Infosys

### About Infosys

Infosys is a global leader in next-generation digital services and consulting. It enable clients in 46 countries to navigate their digital transformation. With over three decades of experience in managing the systems and workings of global enterprises, The Company expertly steer the clients through their digital journey. Infosys do it by enabling the enterprise with an AI-powered core that helps prioritize the execution of change. Infosys also empower the business with agile digital at scale to deliver unprecedented levels of performance and customer delight. Infosys always-on learning agenda drives their continuous improvement through building and transferring digital skills, expertise, and ideas from the innovation ecosystem.

**Infosys**  
Information technology consulting company

[infosys.com](https://www.infosys.com)

Infosys Limited is an Indian multinational corporation that provides business consulting, information technology and outsourcing services. It has its headquarters in Bangalore, Karnataka, India.  
Wikipedia

**Stock price:** INFY (NSE) ₹745.00 +10.30 (+1.40%)  
3 Jan, 3:30 pm IST - [Disclaimer](#)

**CEO:** Salil Parekh (2 Jan 2018-)

**Headquarters:** Bengaluru

**Founders:** N. R. Narayana Murthy, Nandan Nilekani, [MORE](#)

**Subsidiaries:** EdgeVerve, Panaya, Infosys BPM, Infosys Consulting, [MORE](#)

# Cyber Crime Report (An Initiative by) Scholastic Seed Inc.



CyberCrime report can throw a light on upcoming cybercrimes and remedy to it. It can give an awareness about the crime occurred in a society and how to safeguard ourselves and society as a whole in totality. It is a real fact that Cyber crime will never disappear completely, which means businesses have to be extra vigilant in these rapidly changing times. And a CYBERNOMICS worked as a trusted IT partner which can always deploy the right solutions to keep you and your precious resources safe.



## How to report cyber crime India?

Please contact local police in case of an emergency or for **reporting crimes** other than **cyber crimes**. National police helpline number is 100. National women helpline number is 181.

## How do I report cyber crime?

If you are a victim of online **crime**, file a complaint with the **Internet Crime Compliant Center (IC3)** at [www.ic3.gov](http://www.ic3.gov). IC3 is a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar **Crime Center (NW3C)**, the SSA at <http://oig.ssa.gov/report-fraud-waste-or-abuse>

## Where can I report cyber crime in India?

You can register a **cyber crime** FIR at the nearest local police station to **report** them. It is mandatory under Section 154, Code of **Criminal Procedure**, for every police officer to record the information/**complaint** of an offense, irrespective of the jurisdiction in which the **crime** was committed.

## Steps to File a Cyber Crime Complaint

Let's accept it, we have all seen such cases happen with our kith and kin. Losing one's hard earned money to online criminals or seeing a loved one suffer due to a matrimonial scam can be painful and hard to accept.

And the scenario that follows is utter confusion and inability to comprehend the next course of action. Where to file a cyber crime complaint? What are the steps to register a cyber crime FIR? What evidence to provide? How long to wait before following up and so much more!

In the event of a cyber crime, it is really distressing to get a grip on the situation. Worst still, to go through the process of understanding how to file a cyber crime complaint in that grueling moment! We recommend that one should not wait for a cyber crime to strike to be aware of the response mechanism to a cyber offense. The following section shall tell you how to file a cyber crime complaint in India in few simple steps.

1. The very first step to file a cyber crime complaint is to register a written complaint with the cyber crime cell of the city are currently in.

According to the IT Act, a cyber crime comes under the purview of global jurisdiction. This means that a cyber crime complaint can be registered with any of the cyber cells in India, irrespective of the place where it was originally committed.

At present, most cities in India have a dedicated cyber crime cell. The last section of this article shall provide you with the list of cyber cells in India.

2. When filing the cyber crime complaint, you need to provide your name, contact details, and address for mailing. You need to address the written complaint to the Head of the Cyber Crime Cell of the city where you are filing the cyber crime complaint.

3. In case you are a victim of online harassment, a legal counsel can be approached to assist you with reporting it to the police station. Additionally, you may be asked to provide certain documents with the complaint. This would, however, depend on the nature of the crime.

4. Register a Cyber Crime FIR: If you do not have access to any of the cyber cells in India, you can file a First Information Report (FIR) at the local police station. In case your complaint is not accepted there, you can approach the Commissioner or the city's Judicial Magistrate.