****

**An Article on**

Website of an organization-Is it safe and protected from hackers.

BY

MR.KALYAN RAO PEDDI REDDI B.COM (HONS) IN COMPANY LAW & SECRETARIAL PRAC. & BUSINESS ADMINISTRATION & ECONOMICS, ECONOMIC DEVELOPMENT; LL.M (CONSITUTIONAL LAW of India), COMPARATIVE STUDY IN **U.S. American Constitution, Swiss Constitution, FRENCH CONSTITUTION & British Constitution)**,

C.E.O OF KALYAN LEGAL EXCEL CARE SERVICES ONLINE FOR CITIZENS & N.R.Is.

www.legalexcelcare.com

(LAUNCH: 1.1.2018),

Former District & Sessions Judge, now lives at HYDERABAD, INDIA

&%\*$@&

Website of an organization-Is it safe and protected from hackers.

WEBSITE PROTECTION.:

  **National Cyber Security Policy is a policy framework by the Government** [**[1]**](https://en.wikipedia.org/wiki/National_Cyber_Security_Policy_2013#cite_note-http:.2F.2Fdeity.gov.in.2Fcontent.2Fnational-cyber-security-policy-2013-1-1) **It aims at protecting the public and private infrastructure from cyber attacks.**[**[2]**](https://en.wikipedia.org/wiki/National_Cyber_Security_Policy_2013#cite_note-cyber-2) **The policy also intends to safeguard "information, such as personal information (of web users), financial and banking information and sovereign data". This was particularly relevant in the wake of National security Authority (NSA) leaks that suggested the US government agencies are spying on Indian users, who have no legal or technical safeguards against it. Web security and protection defines that it is a complex environment consisting of interactions between people, software services supported by worldwide distribution of information and communication technology**

 **::2::**

## How the ATP safe links feature works

 As part of the Office 365 security stack, the ATP safe links feature helps prevent exposure to emerging threats. ATP safe links protection can be defined for email and for Office 365 ProPlus files (Word, Excel, PowerPoint, and Visio documents) on Windows devices.

| ATP safe links in email | ATP safe links in Office documents |
| --- | --- |
|  | At a high level, here's how ATP safe links protection works for hyperlinks in Office applications (Word, Excel, PowerPoint, and Visio) on Windows:1. People have installed Office 365 ProPlus on their computers running Windows.
	* A user opens a Word, Excel, PowerPoint, or Visio, and signs in to Office 365 Enterprise using their work or school account. The document contains hyperlinks. When the user clicks on a hyperlink in the document, the link is checked by the ATP safe links service. If the link is to a website that is included in a ATP safe link Office documents for a policy that applies to the user, that user is taken to the website.
	* If the link is to a website that is included in the organization's, the user is taken to a warning page.
	* If the link is to a website that has been determined to be malicious, the user is taken to a warning page.
	* If the link goes to a downloadable file and the [ATP safe links policies](https://support.office.com/en-us/article/ATP-safe-links-policies-bdd5372d-775e-4442-9c1b-609627b94b5d) are configured to scan such downloads, the downloadable file is checked.
	* If the link is considered safe, the user ﻿is taken to the website.
 |

## How do we get ATP safe links protection?

The ATP safe links feature is part of Advanced Threat Protection, which is included in Office 365 Enterprise E5. Advanced Threat Protection can also be purchased as an add-on to Office 365 Enterprise E1 or Office 365 Enterprise E3. For more information about plan options, see [Compare All Office 365 for Business Plans](https://go.microsoft.com/fwlink/?linkid=844053)

 ::3::

The ATP safe links feature applies when:

* ATP safe links policies are set up for email and for Word, Excel, PowerPoint, and Visio documents
* How do we know if ATP safe links protection is in place?

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |

 Check the seal of approval

 **You can increase your privacy and security by shopping only at sites and using only services that have been certified by an Internet trust organization. For more information about trust organizations, go to the website,.**

**Note: These seals don't always guarantee that a website is trustworthy. Some unscrupulous websites might display the trust logos fraudulently.**

## 5 signs that a website might not be trustworthy

**Here are five reasons NOT to go to a website:**

1. **You learn about the site or receive a link to it in an email message that was sent by someone you don't know (or by someone in your contact list, but with no explanation).**
2. **The site offers objectionable content, such as pornography or illegal materials.**
3. **The site makes offers that seem too good to be true. This can indicate a possible scam or the sale of** [**illegal or pirated products**](https://www.microsoft.com/en-us/safety/pc-security/piracy.aspx)**.**
4. **You are asked for a credit card number as a verification of identity or for personal information that does not seem necessary.**
5. **You are asked to provide a credit card number on a page that does not start with HTTPS or does not include the lock icon.**
6. **Your website got hacked and blacklisted by Google? This is really bad, you are going to lose your website visitors, and in result your business will lose its credibility. Our security tools will scan and analyze your website every day. Our team will monitor your website 24/7 and if any issue is detected, we will make all necessary corrections to ensure your web site is up and running. Keep your website safe and secure with our complete website security solution.**

**::4::**

**(www.siteguarding.com)**

### Vision

**To build a secure and resilient cyberspace for citizens, business and government and also to protect anyone from intervening into your privacy.**

### Mission

**To protect information and information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threat, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology and cooperation.**

### Objective

###  The Act defines objectives as follows:

* **To create a secure cyber ecosystem in the country, generate adequate trust and confidence in IT system and transactions in cyberspace and thereby enhance adoption of IT in all sectors of the economy.**
* **To create an assurance framework for design of security policies and promotion and enabling actions for compliance to global security standards and best practices by way of conformity assessment (Product, process, technology & people).**
* To strengthen the Regulatory Framework for ensuring a SECURE CYBERSPACE ECOSYSTEM.
* To enhance and create National and Sectoral level 24X7 mechanism for obtaining strategic information regarding threats to ICT infrastructure, creating scenarios for response, resolution and crisis management through effective predictive, preventive, protective response and recovery actions.
* To improve visibility of integrity of ICT products and services by establishing infrastructure for testing & validation of security of such product.
	+ - * 1. ::5::
* To create workforce for 500,000 professionals skilled in next 5 years through capacity building skill development and training.
* To provide fiscal benefit to businesses for adoption of standard security practices and processes.
* To enable Protection of information while in process, handling, storage & transit so as to safeguard privacy of citizen's data and reducing economic losses due to cyber crime or data theft.
* To enable effective prevention, investigation and prosecution of cybercrime and enhancement of law enforcement capabilities through appropriate legislative intervention.

### Strategies

* Creating a secured Ecosystem.
* Creating an assurance framework.
* Encouraging Open Standards.
* Strengthening The regulatory Framework.
* Creating mechanism for Security Threats Early Warning, Vulnerability management and response to security threat.
* Securing E-Governance services.
* Protection and resilience of Critical Information Infrastructure.
* Promotion of Research and Development in cyber security.
* Reducing supply chain risks
* Human Resource Development (fostering education and training programs both in formal and informal sectors to support Nation's cyber security needs and build capacity.
* Creating cyber security awareness.
* Developing effective Public Private Partnership.
* To develop bilateral and multilateral relationship in the area of cyber security with other country. (Information sharing and cooperation)
* Prioritized approach for implementation.
* Operationalisation of Policy