Week 2 Discussion

7 Ways to Protect Your Privacy Online

Delete Cookies: First of all, I know that most of the sites we are visiting they are asking for the cookies. I never looked at how many cookies were stored in my browser. I knew that they use cookies to run faster while we visit. These links, look like they can see what I am doing on the browser. I visit any social media site I never sign out. So form this learn to protect data, Data privacy. I learned from this site about how to secure my data and privacy. Which browser has to use which search engine I can use. Encryption of the data.

Cybersecurity Awareness: Your Checkup Checklist:

This link is all about staying up to date with technology. Always check for windows updates, browser update, and software updates so that if they have any updates related to security, privacy, or protection so our laptop or desktop and another device that I am using is secured against any malware.

This checklist shows you that I am secure from cyber-attacks. Is the computer up to date? A mobile device is password protected? Don’t share a password with others. Don’t share private data with others.

Replay :

The key to dealing with malware is prevention and education. Keep everything, from the security policy to the antivirus protection, as up to date as possible. It's better to avoid downloading any files that originate from someone you don't know or that you find online.

Attacks by a man-in-the-middle  
The most effective approach to avoid MITM attacks is to encrypt data (preventing it from being viewed publicly). This includes making emails, documents, and other material you transmit over the internet only accessible to people who have authorization to see them. There's also the option of enabling certificate-based authentication on all of your company's devices. This implies they'll be the only ones who can see what's being sent.  
Get rid of access assaults. Create the strongest passwords can help. Install protection software that performs a thorough virus scan.

Phishing

Businesses should avoid disclosing personal information to anyone they haven't seen in person or with whom they haven't had substantial internet discussion. Informing employees about any well-known phishing scams. Keeping them as informed as possible will go a long way toward assisting them in detecting a potential threat.

Hello Bansari,

It’s a good approach to secure our data by sharing encrypted files and only giving access to the authorized person only to read the file. The way you can protect your data from being shared publicly. Also, keeping employees updated with phishing scams is the way to secure your company from Phishing scams. Also, any company can secure their data by sharing data using internal networks for sharing important files instead of sharing over the internet. Use a different types of protection like encryption, and authentication to secure their files. Very well explained thanks for sharing.

Hello,

**Key information security mistakes organizations make:**

* **Ignoring the fundamentals:** In most cases, the attacker exploits the underlying weakness in the fundamental components of a security ecosystem. Security professionals' focus gets diverted to the latest and fanciest security solutions. They keep forgetting or neglecting the basics.
* **Lack of holistic approach: Instead** of understanding the root causes for defining corrective action plans, many organizations work to clear only the symptoms that are obvious.
* **Lack of Adequate visibility: Lack** of complete visibility of organizational processes and assets, hence becoming blindfolded with the security risks associated with it.
* **Missing Security in business processes: Organizations** don’t give importance to this element, and Information Security experts focus on security awareness programs and process directly related to information security only. Albeit these are fundamental; similarly significant is the business cycle upgrade with security installation.
* **Ineffective change management:**After designing and deploying the best security for the company and getting audited and certified, if the IT team carries out uncontrolled changes without adequate security controls and audits, then, at that point, it could open up new security openings that sidestep a significant number of the actions carried out till then, at that point.
* **Focus on Production Environment Only and ignore the security of the Test & Development environment:** The sensitive or valuable information may be available in test/development systems or in external storage. Any security compromises of IT frameworks (regardless of creation or test/dev) could be adverse to the organization, as the platform for additional assaults.
* **Lack of data identification and classification:**The absence of efficient classification and monitoring of information, and the dearth of enough importance given to data-centric security.
* **Ineffective policies – Just in Paper! :**Arrangements and methodology become simply static records, and not sufficiently carried out or powerful. While strategies are fundamental for the association, their viability is similarly significant as well. In many cases, consultants or staff do copy-past policies, which were developed for other agencies.
* **Lack of Authority:**Establish an Information Security Function with or without a CISO, who does not have the authority, budget, resources, and reach to ensure end-to-end security. Exactly when CISO is placed in a few unsuitable divisions, with unfit uncovering lines, and without the right power, Information Security gets the least importance and the last need in hierarchical activities and objectives.
* **Uncontrolled or Unrestricted Network Traffic Management:** Uncontrolled and unmanaged outgoing traffic (no visibility too) with ineffective monitoring could end up in significant security incidents. Generally speaking, associations will quite often safeguard from undesirable approaching traffic however disregard the active traffic.

Having the knowledge of common information security mistakes and how to fix them will be helpful in understanding the organization's vulnerabilities and supporting them with the fixes. It can also be useful for start-ups as checkpoints to consider while building policies, security firewalls, and other security-related stuff.

**Few ways to protect your privacy online:**

* Delete Cookies
* Log Out of Social Media Sites While You Browse the Web
* Change Your Smartphone’s Privacy Settings
* Skip Store Loyalty Cards
* Employ Advanced Online Tools
* Opt-out of Data Broker Collection
* Do a Digital Check-up

I didn’t have much idea about privacy protection previously. By following these steps I can reduce the data that gets collected anonymously by the websites related to me.

**Five worst security practices found in businesses:**

* failing to enforce policies
* ignoring new vulnerabilities
* relying too much on technology
* failing to screen job candidates
* assuming that security experience alone is enough for IT staff to maintain or lead the security team of an organization

Having a thought regarding some unacceptable practices in the associations/organizations will help in understanding the security-related issues. We can suggest/fix the mistakes when we see these problems in the business.

Hello Manikanta

Nice Explanation of security mistakes made by any organization. Yes, most of the time companies do not take more look at traffic. I never knew that thing even a company can miss for protection and privacy of the data. I know some of the policies that the company has to follow and also the employee, like blocking USB Slote from the system, and sharing data It’s a good key point on how to protect online privacy. Thanks.