“SEE YOURSELF IN CYBER”

SEE YOURSELF IN CYBER

This year's campaign theme — "See Yourself in Cyber" — demonstrates that while cyber security may seem like a complex subject, ultimately, it's really all about people. This October will focus on the "people" part of cyber security, providing information and resources to help educate the public, and ensure all individuals and organizations make smart decisions whether on the job, at home or at school – now and in the future. We encourage each of you to engage in this year's efforts by creating your own cyber awareness campaigns and sharing this messaging with your peers.

5 THINGS YOU CAN DO

Throughout October, we will highlight key action steps that everyone should may take:

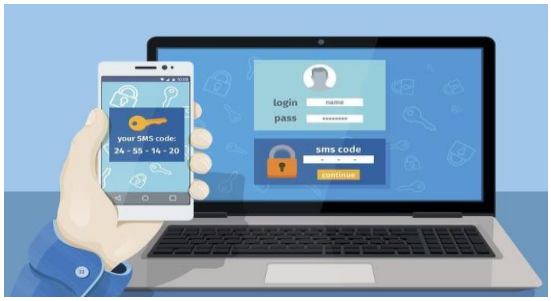
- Enable Multi-Factor Authentication.
- Use Strong Passwords.
- Recognize and Report Phishing.
- Update Your Software.
- Be Cyber Security aware on social media.

YOUR ROLE

When we say See Yourself in Cyber, we mean see yourself in cyber no matter what role you play. As an individual or consumer or entrepreneur, take basic steps to protect your online information and privacy.

ENABLE MULTI-FACTOR AUTHENTICATION

- It goes by many names. Two Factor Authentication (2FA.), Multifactor Authentication (MFA).



- They all mean the same thing. Opting-into an extra step when trusted websites and applications ask you to confirm you're really who you say you are.
- Your bank, social media network, school, workplace all they want to make sure you're the one who is accessing your information.
- So, application is taking a step to double check. Instead of asking you for a password, which can be reused, more easily cracked, or stolen, they can verify it's you by asking for two forms of information:
  - ✓ They'll ask for something like a PIN number or your sister's middle name, or other information.
  - ✓ Something you have like an authentication application or a confirmation text on your phone.
- The second step is a lot harder for a hacker to fake. So, we may use the multifactor authentication (MFA/2FA) with all over applications.
- We may start with email account, then financial services, then social media accounts, then online stores, and don't forget for gaming and streaming entertainment services also.

USE STRONG PASSWORDS

- Did you know the most common password is “password”? Followed by “123456”? Using your child’s name with their birthday isn’t much better.

- Picking a password that is easy is like locking your door but hanging the key on the doorknob. Anyone can get in.

- Here are some tips for creating a stronger password. Make sure it’s:

  - ✓ **Do not use sequential numbers or letters**
    For example, do not use 1234, qwerty, jklm, 6789, etc.

  - ✓ **Do not include your birth year or birth month/day in your password**
    Remember that cyber criminals can easily find this information by snooping into your social media accounts.

  - ✓ **Use a combination of at least eight letters, numbers, and symbols**
    The longer your password and the more character variety it uses, the harder it is to guess. For example, *M0l#eb9Qv?* uses a unique combination of upper- and lowercase letters, numbers, and symbols.

  - ✓ **Combine different unrelated words in your password or passphrase**
    This makes it difficult for cyber criminals to guess at your password. Do not use phrases from popular songs, movies, or television shows. Use three or four longer words to create your passphrase. For example, *9SpidErscalKetobogGaN*.

- ✓ **Do not use names or words found in the dictionary**
  Substitute letters with numbers or symbols to make it difficult to guess the password. Or deliberately use spelling errors in the password or passphrase. For example, *P8tty0G#5dn* for "patio garden."

- ✓ **Use a password manager to store your passwords**
  Do not store your passwords in a document on your computer. Make sure you're using the password manager tool provided to you by the IT/support team to store all professional and personal passwords.

- ✓ **Do not reuse your passwords**

  Every device, application, website, and piece of software requires a unique and strong password or PIN. Remember, if a cybercriminal does guess one of your passwords, they will use this to attempt hack into all of your personal and professional accounts.

- Remember never to share your passwords with anyone. This includes your colleagues, the IT/support team, customer service/helpdesk personnel, family members, and friends.

- Make sure you're not recycling the same password across all your apps and websites.

- You can use a password manager to store all of your passwords. That way you don't have to remember them all! If you go this route, make sure your master password is strong and memorable, and secure your password manager account with MFA.

RECOGNIZE AND REPORT PHISHING

Phishing is a form of fraud where a scammer attempts to have you reveal personal financial or confidential information by posing as a reputable entity in an electronic communication. Many scammers try to bait you by urging you to open an attachment or to respond immediately by clicking a web link that appears official (with all the familiar logos or corporate phrases). Even if the request looks genuine, be skeptical and look for these warning signs.

How to Recognize Phishing Attempts

- ✓ The message is unexpected and asks you to update, confirm or reveal personal identity information (e.g., full Social Security Number, account numbers, NetID, passwords, protected health information).
- ✓ The message creates a sense of urgency.
- ✓ The message may include an unusual “From” address or an unusual “Reply-To” address, it may even be a compromised address. If you receive an email from someone you don’t normally communicate with, pay special attention to the other ways to detect its legitimacy.
- ✓ The message includes links that don’t match the name of the organization that it allegedly represents
- ✓ The message includes grammatical errors (although scammers are getting better at this).
- ✓ The message is unexpected and offers an unbelievable job opportunity with great salary and perks.

Report Phishing

If any user gets indicative type of phishing mails or received phishing mail or otherwise, then user should report immediate on e-mail id: cyberreport@itbp.gov.in for support. (like for changing credentials, formatting of system, creating alert for others, etc.)

UPDATE YOUR SOFTWARE

Open your laptop/desktop/ device and see this little pop-up window saying “update your software”. Usually, people will try to ignore this notice by clicking the “remind me later.” But you shouldn’t do this. Always choose to update your software no matter how long it takes. These software updates are necessary to keep your device updated, secured, and safe.

5 Amazing benefits of software update:

- ✓ **Discover Computer Bugs and Viruses**
  When you update your software, you discover viruses and bugs that have been with your device for quite some time. Through updates, it allows you to remove the computer bugs and viruses to prevent your software and devices from getting crashing.

- ✓ **Cure Security Flaws**
  Another benefit of getting your software updated is that it lets you cure security flaws.
  What is a security flaw? This is a software vulnerability or security hole or weakness that is in your software and operating system. Without updating your software, hackers can easily get into your device by writing code to target security flaws. This code is malicious software that can exploit and infect your device. Worse is that it steals every data you saved on your device.
  Through a software update, it lets you 10x ensure that hacking can never be possible.

- ✓ **Protect Cyber Data**
  You might have a lot of information and important document on your computer and they are valuable to you because this information forms part of your work and life. However, without updating your software, cyberhackers can easily destroy and encrypt your data. And the worse part, you might pay a dime to get this encryption back. So, updating your software gives you a great chance of protecting your cyber data from getting hacked and destroyed.

- ✓ **New and Faster Software**
  The best part of getting your software updated is that– new and faster software. What does it mean for you? No more crashing, no more lagging, and no more hacking plus you'll be productive in your work. You could also ignore those annoying reminders of updating software and you'll start having the most secured data.

- ✓ **Prevent Passing Bugs and Viruses to Other Devices**
  So, we've discussed the benefits of a software update, and all of them are mostly about you. But there are other people too. If your device has a virus in it, you can pass it on to your friend's devices, and worse, it might damage their computers. That's why it's essential to keep your software and systems updated.

BE CYBER SECURITY AWARE ON SOCIAL MEDIA

Social life that helps us connect to friends, family, colleagues, or others. We have witnessed how the advent of social media platforms like Facebook, Twitter, and WhatsApp brought a revolutionary change in how we use the internet for personal and professional purposes. Even though there are security settings among social media platforms, people with mischievous intentions still find a way to gain access to sensitive personal information

ISSUES INVOLVING CYBERSECURITY FOR SOCIAL MEDIA

- ✓ **Privacy of Data**
  Users share their personal information on social media, which can cause privacy breaches. For example, a user's information can be viewed by everyone if the user's default setting is public.'

- ✓ **Data Mining**
  We all leave a data trail behind on the internet. When someone creates a new social media account and provides details such as date of birth, name, location, personal habits, and without our knowledge, all these data are leveraged and shared with third-party for targeting advertising. It can cause security concerns as third-party may collect real-time updates on the user's location.

- ✓ **Virus and Malware Attacks**
  Malware and viruses quite often find a way to the computer system through annoying ads. Once gaining access to the network, the attacker steals confidential data or causes complete disruption to the computer system.

- ✓ **Issues involving the use of 3rd Party Applications**
  Most of the applications nowadays ask permission from users to access personal information's such as contacts, picture, and current geographic location before installing, and some of these applications which are running in the background might download malware on the user's phone or smart devices without their knowledge.

- ✓ **Legal Issues**
  There are legal risks associated with the use of social media**,** like posting offensive content towards any individual, community, or country.

RISKS & CHALLENGES

- ✓ **Identity Theft:** As millions share their personal information for getting registered in one or more social media platforms, these data become vulnerable as hackers and identity thieves use this information's to reset passwords, apply for loans, or other malicious objectives.

- ✓ **Romance Scams:** A romance scam is a fraudulent scheme in which a swindler pretends romantic interest in a target, establishes a relationship, and then attempts to get money or sensitive information from the target under pretenses.

- ✓ **Whistle-blower**: People are often impulsive on social media; they show their vexation with their colleagues or bosses without thinking. They may deliberately reveal sensitive data in their posts, which can cause significant damage to the reputation of the organization.

- ✓ **Cyber Stalking**: It refers to harassment over the internet. Cyberstalks harass victims on social media by sending unpleasant and lewd messages. They morph photos of victims

and circulate them on social media, alleging rumours making the victim's life unbearable.

- ✓ **Cyber Bullying:** It refers to bullying through the digital medium. It can take place on social media, gaming platforms, messaging platforms, etc. It is aimed at scaring, shaming, or annoying the targeted victim.

- ✓ **Cyber Terrorism:** Nowadays, social media is also used to facilitate terrorism-related activities. It can support, promote, engage, and spread terrorism propaganda like incitement to terrorism, recruitment, radicalizing training, and planning of terrorist attacks.

SOLUTIONS ON SOCIAL MEDIA CYBERSECURITY

- ✓ Creating strong passwords is the primary option to ensure the privacy of your information.

- ✓ Ensure passwords are complex, including upper & lower case, numbers, and special characters. It should be memorized and never be written on paper.

- ✓ We need to be sensitive in what we upload/share in our social networking accounts and avoid sharing personal information like date of birth, social security details, phone numbers, names, and pictures of family members.

- ✓ Use security and privacy options provided by social media platforms viz: 2-factor authentication system, access control.

- ✓ Connect our devices only to authorized wifi access, use privacy options provided by various mobile operating systems, use auto-lock features, and download apps only from authorized app stores.

- ✓ Keep the operating system updated with the latest patches, turn-on the firewall, and avoid installing cracked software.

- ✓ Ensure our antivirus is updated and scans are performed frequently.

- ✓ We need to be smart using the internet and avoid visiting untrusted websites; referral links to visit websites are never to be clicked; instead, type in the browser's URL address.

- ✓ Care needs to be taken to accept friend requests only from people we know and block those who post upsetting content or comments.