How to #BeCyberSmart and #CyberAware for a #CyberSecure world?

It is October. Yes, this is Halloween month but there is something else that we IT people look forward to. It is Cybersecurity Awareness Month and as a special treat for our readers, we decided to celebrate it by preparing a guide to #BeCyberSmart. Ghosts may be scary, but not being cyber aware? It is a nightmare. At Hexnode, we take cybersecurity pretty seriously. We even ended up throwing one of the biggest cybersecurity events of the year in September – HexCon21.

The Cybersecurity and Infrastructure Security Agency (CISA) has put forth its own suggestions for us to focus on this month:

1. Be Cyber Smart
2. Fight the Phish!
3. Explore. Experience. Share.
4. Cybersecurity First

Let's start from the basics

Who exactly needs cybersecurity? The simple answer to that is – everyone. We live in a connected world, and every single endpoint pose a security risk if they are not properly protected.

> "Cybersecurity begins when the employee first turns on the device
> – Dovell Bonnett, CEO at Access Smart at HexCon21

The hard truth, the truth that no one really likes to accept, is that the weakest link in cybersecurity is often the users themselves. The reason is a no-brainer. Users tend to prioritize convenience over security. To put the users in charge of securing their own devices is like giving a loaded gun to a toddler for self-protection. In other words, it doesn't make sense. Devices cannot be left unmanaged and that's what we are going to talk about.

Did you know?

- Almost 67 percent of the world population are mobile users while around 61 percent of the world population are on the Internet.
- In 2021, data breach costs rose from USD 3.86 million to USD 4.24 million.
- More than 20 percent of the breaches were due to compromised credentials like passwords1.
- More than 95 percent of working-age internet users spend their time on social networks and messaging services.
- Small businesses are the target of around 43 percent of cyberattacks. There is almost a 400 percent increase since the pandemic began.

Now that we have scared you enough with the statistics, let's move on to the part where you learn to outsmart the attackers.
A good rule of thumb is: Before you connect IT, protect IT. Now, how can you do that?

Building a solid foundation

If you have a good cybersecurity framework in place, your work is mostly done. Broadly, we can classify the whole cybersecurity lifecycle into five steps:

1. Identify
2. Protect
3. Detect
4. Respond
5. Recover

Each step comes with a different set of outcomes. You know you have a good cybersecurity framework in your organization if you have implemented all five functions in a comprehensive manner.

Identify

Let me break it down for you in simple terms. If you do not know what to protect and what the risks are, the whole cybersecurity lifecycle is meaningless. What do you need to identify?
First of all, you need to have an exact idea about all the assets in your organization. As we discussed before, each endpoint contributes to the attack surface unless properly secured. For instance, Hexnode admins can see all the enrolled users and devices in their portal. Tracking the assets is easier if you can see them all in one place.
Once you know what to protect, you need to identify the possible risks. Premeditated actions would be a real thorn in the flesh for attackers. Why make their lives easier, right? If it is a healthcare organization, possible risks would include stealing patient information, hacking the mHealth apps or devices that result in direct malfunction, and so on. Similarly, if it is an educational institution, the student data could be a target. For governmental organizations, there is a multitude of possible risks – data leakage being the most important one.
Make a list of possible threats and assess the level of importance for each of them.

A generic threat list for you

- Phishing
- Network spoofing
- Data leakage

- Ransomware
- Malware
- Stolen/lost devices

Protect

You have the list of threats. What to do next? It is pretty obvious – you have to take measures against the threats identified. While you can never be a cent percent sure that you are protected, you can take measures to make the job of attackers very very hard. All talk and no work make cybersecurity a tough nut to crack. Let's take a look at a few measures you can take in your organization.

Security training for employees

Nothing beats awareness. It's the whole reason why we are celebrating Cybersecurity Awareness Month. Educate your workforce with basic security protocols they should follow on an everyday basis.

P@$$w0rd Security

> "All cybersecurity experts I interviewed agreed on one thing – Cybersecurity is not just a tech problem. It is a human problem too. 85-95 percent of all successful data breaches involve some human element.
>
> – Donald Allen, Bestselling author and cybersecurity expert at HexCon21

It sounds basic but it is literally the first level of security against cyberattacks. Educate your employees. Make them aware of the minimum standards they need to follow while securing their devices and accounts with passwords. Encourage them to prioritize security over short-term convenience.

Some tips for users

- Say goodbye to the common passwords. If you have 123456 or your pet's name as your password, you are just inviting attackers with open arms.
- Stop using the same password for different accounts.
- Enable two-factor or multi-factor authentication whenever possible.
- Do not reuse passwords.

What can the admins do?

Hexnode admins have some good options at their disposal to enhance password security in managed devices.

- Enforce complex passwords. Create strong password policies with high complexity requirements. It is a given that complex passwords are harder to crack. Ensure that the users have to set a password of minimum length with special characters and numbers thrown into the mix.
- Everything expires. Even passwords. Set an expiry date for the passwords. The users must update the password regularly to avoid any risks.
- Old passwords are history. Do not let the users reuse old passwords. Restrict the users from doing so with Hexnode's password policy.
- Too many wrong attempts? Lock them out. If the user is repeatedly giving a wrong password, it is possible that the user is not legitimate. With Hexnode, you can configure a policy to wipe the device automatically after a specified number of failed attempts.

Securing networks

A good cybersecurity strategy would include enterprise network security. The importance of securing corporate networks cannot be downplayed at all. The whole organization can be brought down if the networks are compromised. Let's have a look at how admins use Hexnode for network security.

- Wi-Fi: Push the corporate Wi-Fi configurations remotely with Hexnode. The users would be able to connect to the network automatically without entering the password.
- VPN: I know, VPNs are becoming more and more obsolete. However, if your organization is not evolved enough to employ Zero Trust security principles, you would have to fall back on VPNs to provide security. Remotely configure and deploy VPN to your managed devices with Hexnode.
- SCEP: Configure SCEP to enforce certificate-based authentication to fight the security threats caused by accessing work emails, Wi-Fi, VPN and more.
- Global HTTP proxy settings: Set up proxy for devices globally with Hexnode to ensure that all HTTP network traffic passes through it.
- Web Content Filtering: Visiting untrustworthy websites is a sure way of increasing the attack surface. Set up web content filtering policies to prevent the users from visiting potentially malicious websites.

Managed devices with managed apps

- Not all apps need to be present in the work devices. In fact, some apps shouldn't be installed at all. Apps often require many permissions to be installed and we give those permissions easily without even bothering about whether it would open a new access point for the attackers.

- Have control over the installed applications. Choose the applications to be installed in the devices and deploy those applications. Uninstall the applications that aren't required. Use blacklisting and whitelisting to ensure that no errant apps are present in the devices.
- Manage app permissions and configurations. Decide the app permissions and configurations even before the apps are installed in the device.
- Isolate work apps from personal apps in BYOD scenarios. Work and personal data should be separated. Segregate work and personal apps and data with Hexnode so that the two worlds do not mingle even in a single device.
- Create a custom app store for users. Prevent the users from going to digitally unsafe places to get the apps they need. Provide them with all the apps they need with Hexnode's custom app store.

Phighting email phishing with Hexnode

Bypass email phishing attempts by taking the following measures:

- Configure managed email domains. Employees can open emails or download attachments only if received from managed domains.
- Disable clipboard (copy and paste) for emails.
- Ensure that the emails are not opened from unmanaged applications.

Detect

Even if you are cyber smart, it is always possible that your attackers are smarter. It is important to detect any possible attacks as soon as it occurs to minimize the damage. For instance, Hexnode admins can see if any of the devices are not checking in to the portal from the dashboard itself. They can also check the reports to ensure there are no anomalies. Develop a strategy for timely detection of any cybersecurity incidents in your organization.

Respond

The cybersecurity incident has happened. Now, the only thing you can do is to contain the attack and reverse the effects if possible. For instance, you could do a remote wipe of the victim's device. Manage communications with the users and other admins throughout the response process. Once the incident is resolved, move on to the recovery stage.

Recover

While formulating the recovery strategy, it is important to include the scope for improvement and the lessons learned from the previous experience. Restore all the assets affected by the cybersecurity incident and attempt to go back to normal operations.

Of course, this has to be done after taking measures to ensure the incident doesn't happen again.

Do your part. #BeCyberSmart.

Both private and governmental organizations worldwide are recognizing the importance of cybersecurity. Just a week ago, President Biden signed the K-12 Cybersecurity Act to enhance the cybersecurity of K-12 educational institutions. That wasn't all. Google launched its very own Cybersecurity Action Team to support governments, enterprises, and SMBs for increased cyber resilience. Is cybersecurity only meant to be the responsibility of the big shots? Certainly not. We cannot be cyber security as a whole until each and every one of us does our part. Just like CISA's slogan says, "Do your part. #BeCyberSmart."