IPSYSTEMS,INC.
ALL ABOUT DATA SECURITY

AWARENESS IS THE FIRST STEP

It’s Time to Make Employees Care About Cybersecurity

To improve security across your organization, you have to ensure that your employees are aware about what cyber and data security is. It is no doubt that they are your greatest asset, however, they can also be your greatest liability.

Showing your employees the importance of cybersecurity is easier said than done - especially when they have their own deadlines to beat. But as new threats emerge, regular security trainings must be implemented on an enterprise-wide level.

The argument for educating employees on cybersecurity is simple: If your employees don't know how to recognize a cyber attack, how do you expect them to avoid it, report it, or remove it?

So, what are the steps that you can take to help improve your employees’ cyber hygiene?

By enabling your employees to know what security threats are, how they might present, and what procedures to follow when a threat is identified, you're strengthening the most vulnerable link in your cybersecurity chain.

Therefore, cybercriminals are more likely to move on to someone else’s waters and leave yours alone.

Here are some steps to help you train, inform, and make your employees care more about the role they play to strengthen the cybersecurity of your organization.

01 Create a comprehensive Cybersecurity Training Plan

The first step in ensuring that your employees are onboard with your cybersecurity strategy, there should be an organized training plan in place for employees. It must also be updated as necessary and accessible to employees who might want to read it from time to time.

02 Include a cybersecurity training during onboarding

As you hire new employees, it would make a lof of sense to have them attend a cybersecurity info session as well. It's never too early to help them learn what a good cyber hygiene is. Remember that they will gain access to accounts, customer data, and other sensitive information.

03 Educate employees on Data Privacy Policies

Remind employees, both tenured and new, about your company's Data Privacy Policy. Let them know that just because some data are accessible to them, doesn't mean that they can freely use it. For example, a list of contacts who have opted out from receiving any further newsletters, if an employee emails them, they are violating this privacy.

04 Reiterate that no one is safe from attacks

Make it clear to them that aside from having all the cutting-edge cybersecurity solutions, awareness is still the most important part of preventing attacks. Even large corporations are not safe from these cybercriminals, therefore, it's not a question of "IF" but "WHEN" it happens they should know how to react quickly to block the attack and minimize damage.

05 Show them the benefits of learning cybersecurity

If you educate them on the importance of cybersecurity, you can also show them what's in it for them. What they will be learning during the training can also be applied to their personal online safety. Communicate that this information can be used to their advantage, not just the company's interest.

06 Keep them updated on the latest threats

In order to help employees improve their awareness on their online security, you should send regular updates on the newest cybercrime techniques, scams, viruses, malware, software updates, and other cybersecurity information.

07 Invite cybersecurity awareness and training experts

To further establish the seriousness of data breaches and cyber attacks, it would be helpful for your entire organization to have professionals in the field to conduct training, lay out the basics of online security, and teach specifics skills to your employees.

08 Have cyber attack drills or simulations

As they always say: "Experience is the best teacher", which is why it's important to let employees apply what they have learned thru simulations set up by your internal security team. These drills should be based on specific job roles and must focus on attacks that employees could receive. It will also allow them to identify their reaction time, the move they make, and finally see what areas they can improve at.

09 Normalize talking about Data Ethics

Make it a habit to normally talk about data integrity. When your employees think about any data as something that represents a person, family, or organization, data breaches and leaks are less likey to occur.

10 Communicate clearly and concisely

Stay away from long emails and memos. A lot of employees will just skim the first couple of sentences before deleting it. Instead, get straight to the point and you can also spice it up a bit. You can create short videos, send out infographics, or post short reminders in areas where it could be easily seen.

Having an efficient employee awareness training enables your organization to effectively reduce insider threats. The combination of expert cybersecurity training and world-class security solution is the ultimate weapon against cybercriminals.

LET’S DO A RECAP!

WE’D BE HAPPY TO ANSWER ALL YOUR CYBERSECURITY CONCERNS

☎ +63 (2) 8638 - 3264 ✉ inquiry@ipsystems.ph www www.ipsystems.ph