THE NATIONAL CYBERSECURITY SOCIETY

Employee Cybersecurity Fundamentals

As a small business owner, you may recognize the importance of cybersecurity to protect your company. Whether your employees are entering data into your systems, sharing data with other partners or just ringing up a sale, your employees are a critical component in using IT effectively and keeping your business safe.

According to a study of 1000 small business owners and C-Suite executives, conducted by Shred-it in June 2018, 42% cited human error or accidental loss by an employee as the cause of a data breach at their organization.

With that in mind, the NCSS has developed the top 10 training cybersecurity fundamentals for your employees to master. Employees should be trained on these components as part of their on-boarding process and as a minimum provide a refresher annually.

TIP 1: Personally Identifiable Information (PII)

All employees should be trained on what is PII - how to recognize it, how to handle it, how to store it and who it can and can't be shared with.

TIP 2: Phishing

Employees should be trained on how to identify a phishing email and what to do if they clicked on a link. There are plenty of free resources on the Internet to use in teaching employees about this scam. Conduct a phishing exercise once a year.

TIP 3: Passwords

Employees should know what constitutes a strong password, not to share them with others, not to reuse passwords and how often to change them. If possible, encourage all your employees to use a password manager and enable two factor authentication on all business applications.

Did you know?

- √ There are fact sheets and how to guides on our website that go into detail about each cyber fundamental in this guide
- √ 90% of all cyber incidents could have been prevented through good password management and phishing awareness
- √ If you company has been harassed on social media the SBA has a guide called "Social Media Cyber-Vandalism Toolkit"
- √ Some MSSPs provide VPN services
- √ A good way to reinforce these cyber fundamentals is at your weekly staff meeting.

Still have questions, need help?
Contact us at our "**Ask-an-Expert**" service,
web@thencss.org or visit us at the link below.

Employee Cybersecurity Fundamentals continued...

TIP 4: Social Media

Instruct your employees on the use of social media both at work and when they leave work. Ensure that all employees are cognizant of what can and can't be shared on social media.

TIP 5: Internet Usage

Establish an Internet Usage policy for your employees and communicate the rules of the road once a year. Ensure that your employees are alert to look out for bogus websites, non-HTTPs sites, and the dangers of downloading files off the Internet. Define how much time can be spent on the Internet for their personal use while at work.

TIP 6: Physical Security

Educate all employees on how to keep the business safe from intruders due to doors left unlocked. If you have a uniform policy or a name tag policy for employees - make sure they understand it is part of the security of the business, so employees can be readily identified from customers.

TIP 7: Trash

Inform your employees what can and can't be thrown in the trash. There have been many data breaches where sensitive data was thrown in the trash. Instruct employees where documents can be discarded safely, like a burn bin.

TIP 8: Social Engineering

Inform your employees to be on the look-out for unusual phone calls or emails from fraudsters trying to gain sensitive data about your business. When in doubt, hang up or look it up!

TIP 9: Incident Reporting

Ensure your employees are informed that they are often the first line of defense against a cyber heist. If something doesn't seem right, encourage them to report it. *"If you see something, say something."*

TIP 10: Teleworking

Ensure your employees understand your policy on working from home or the road. If teleworking is allowed, ensure they use a VPN connection to access your business resources.

Still have questions, need help?
Contact us at our "**Ask-an-Expert**" service,
web@thencss.org or visit us at the link below.