Cyber Security for Employees

A 2005 study[1] on security awareness training found one in ten workers confessed to downloading content at work they should not, with 62 percent admitting they have a very limited knowledge of IT security. Education is crucial in helping protect against intellectual property loss, which can cost United States companies up to $250 billion annually[2]. The following tips and guidelines can help protect computer systems against unauthorized access or attack:

Create Strong Passwords

Creating strong passwords can seem like a daunting task. Today, "password" and "12345" are still among the most commonly used passwords. The following tips can provide tools to create strong and memorable passwords.

- All passwords should be the strongest one can use and remember.
- Strong passwords are at least 8 characters long and use combinations of uppercase and lowercase letters, numbers and punctuation.
- Strong passwords contain words typically not found in a dictionary.
- Adding emoticons if possible can make a password more memorable and can boost strength.
- Do not use the same username and password on multiple websites. Hackers can find that information and use it to access information on many other sites.

Do not open unsolicited or unknown emails

When dealing with unsolicited, unknown, suspicious or cloning emails it is imperative to proceed with caution and go straight to the source to verify information.

- Often in these emails the senders wants the recipient to click on a link that will install malevolent software, known as malware, onto the computer.
- The email may have a provocative subject line, logos from a well-known company or use the return address of an acquaintance.
- If from a company, verify the email address before opening any links or attachments.
- If clicking on a link or open an attachment in an email is required, make sure antivirus software is up-to-date.
- Save files to the hard drive, scan them with the antivirus software and then open the file.

Take precautions with mobile devices

More employees are using mobile devices to access sensitive data, creating additional opportunities for data breaches. When using mobile devices for business, make sure that they are kept secure.

- Always keep mobile computers and devices close when traveling until they can be locked up in a secure location.
- Protect all information with a strong password.
- Encrypt all confidential or personal information.
- Ensure important data is backed up, as it will be lost if a device is lost or stolen.

Leadership for a Safe and Secure Indiana

Checklist

Passwords

- ☐ Change passwords regularly
  - ☐ Computers
  - ☐ Email and social media
  - ☐ Other online accounts
  - ☐ Mobile devices
- ☐ Use strong passwords
  - ☐ Create password with at least 8 characters
  - ☐ Include emoticons if possible in passwords
  - ☐ Do not use the same password for multiple sites
  - ☐ Do not use names, pets or birth years in passwords

Regularly

- ☐ Lock computers when leaving the area
- ☐ Back up important documents
- ☐ Update antivirus software on all devices

Always

- ☐ Save files to hard drive and run through antivirus software
- ☐ Remember passwords, rather than writing them down
- ☐ Keep devices locked up while traveling
- ☐ Stay informed on latest risks
- ☐ Stay vigilant about good security practices

[1] The Important of Security Awareness Training
http://www.sans.org/reading-room/whitepapers/awareness/importance-security-awareness-training-33013

[2] Net Losses: Estimating the Global Cost of Cybercrime visit
http://csis.org/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf

Leadership for a Safe and Secure Indiana

Visit
GetPrepared.in.gov