Cybersecurity Awareness Checklist

LMGsecurity.com

Hackers steal millions of dollars and confidential information daily. Attackers send phishing emails to random employees. When an employee clicks the link, the computer is infected with malware that monitors activity and captures banking credentials, confidential files and other information.

You can protect your organization online by taking a few simple precautions. Here are 14 things you can do to help keep your organization safe.

1. **Think Before You Click** - Phishing emails & social networking sites may contain links to infected websites that may cause your computer to be hacked. Think before you click!
2. **Beware of Fraudulent Web Sites** - Scammers make fake websites that can trick you into typing your password or financial information. Ensure the web address is EXACTLY what it should be.
3. **Don't Respond to Scammers** - When you receive emails or phone calls that may be scams, don't respond. If the request might be legitimate, call a number you already have in your records.
4. **Pick Strong Passwords** - Choose a password that is long (at least 14 characters). Never re-use personal passwords for work, or vice versa.
5. **Never Tell Anyone Your Passwords** - Don't share your passwords with anyone-- not friends, co-workers, vendors, or even IT staff.
6. **Use Antivirus and Keep it Up-to-date** - Install a well-known antivirus software, and keep it up-to-date. That way your computer will be protected from known viruses.
7. **Update Your Software** - Keep your software up-to-date. New software updates include new security "fixes" that can save you time and hassles.
8. **Only Use Trusted Software** - Attackers want their software installed on your computer. They disguise it as a utility or fun game. Don't install software unless you have formal approval.
9. **Secure Your Mobile Device** - Treat your phone, laptop or tablet like a desktop computer. Use a passcode and install antivirus when available.
10. **Be Hip, Encrypt** - Lock up your sensitive data. Encrypt confidential emails, files, USB thumb drives, laptops, and other valuable information.
11. **Hang On to Your Data** - Don't upload data to the cloud, copy it to USBs or email it to personal accounts without explicit permission. Keep your work and personal accounts separate.
12. **Remember: Computer Use at Work is Not Private** - Your organization may monitor your web surfing, email use, computer activity, and more.
13. **Stay Informed** - Know your organization's policies for detecting and reporting phishing attacks and other suspicious behavior.
14. **Be a Hero** - Alert the right people in your organization when you are suspicious of an email or web page or If you clicked a link that you should not have clicked.