SAFETY FOCUSED

Presented by

October 2019

First Aid for Cut and Puncture Wounds

The risk of a cut or puncture wound is a danger in almost every workplace, regardless of industry or location. Whether your job is to handle sharp objects in a factory setting or you are just in an office with scissors, there's always the chance of an injury if you're not careful.

Avoid cuts and puncture wounds, or at least keep them from becoming severe injuries, by remembering these things:

- **Don't take shortcuts**—Stay alert and pay attention to the task at hand. Use proper protective equipment and stick to standard safety procedures.
- **Stay calm**—If you are injured, notify your supervisor and don't panic at the site of blood. If the wound is to an arm or leg, try to raise it above your heart to slow the bleeding.
- **Avoid infection**—Clean the wound with soap and clear water. If necessary, remove debris from the wound using tweezers cleaned with alcohol and then apply an antibiotic cream or ointment. If you have not had a tetanus shot in the past five years, get a booster shot within 48 hours of the injury.
- **Dress it up**—Cover the wound with a bandage or, if necessary, get stitches.
- **Let it heal**—If bandaged, change the bandage once a day or whenever it becomes wet or dirty. A cut that needs stitches should be treated within six hours, unless it is on the head or face, in which case it can be stitched up to 24 hours after the injury.
- **Keep watch**—Check the wound regularly to make sure that it is healing. See a doctor if you notice any redness, increased pain, drainage, warmth or swelling.

Consult a medical professional for more information on managing and recovering from cuts and puncture wounds.

> **"Stay alert and pay attention to the task at hand. Use proper protective equipment and stick to standard safety procedures."**

hierl

Cyber Security Tips for Employees

Cyber safety isn't just a job for your IT department or contractor. Cyber attacks and data breaches have become far more common and far more costly in recent years.

Protect yourself and your organization by remembering these tips:

- **Don't go phishing**—Phishing emails are often sent from an address that looks like it can be trusted or like it is from within your own company. Do not open any attachments or click any links within an email unless you are certain the sender can be trusted.
- **Use strong passwords**—Use a variety of passwords that have a mix of capital and lowercase letters, numbers and special characters. Change your passwords periodically and don't leave them written down for others to find.
- **Follow software guidelines**—Do not install unauthorized software on your company devices, and make sure to keep authorized software updated.
- **Keep your devices safe**—Not all data breaches happen over the internet. Company data can also be compromised if you misplace your device or if an unauthorized person is allowed to enter your office.
- **Be careful with connections**—Beware of public Wi-Fi networks. Use password-protected connections and double-check the spelling of the network to avoid slightly misspelled fakes. Use your company's VPN when possible.

With potential cyber threats coming from many different directions, it falls on each and every employee to be cautious and do their part in keeping your company safe.

According to a 2018 Ponemon Institute study, **27%** of data breaches are caused by negligent employees or contractors.