1. **What is phishing?** *Phishing* is a fraudulent attempt to obtain sensitive information by acting as a trustworthy resource in an email communication. Do not react immediately. Take a few minutes to call the bank or call your boss to verify that email.
2. **What damage can phishing do? Isn't it just a virus?** Phishing can give someone access to all the information on your computer—passwords, banking accounts, credit cards and any other information you have stored in your computer. Beyond just your desktop or laptop, a hacker can gain access to your company network and cause substantial damage not only financially, but to the company's reputation.
3. **Don't I just look for misspellings or odd links?** Over time, phishing attacks are getting more sophisticated. It used to be that phishing attacks were easily spotted by looking for misspellings or errors in grammar. What if the email comes from what looks like your bank with a recognized logo, or an email from your boss asking you to wire money? Many people click!
4. **How can awareness training help?** With training, users begin to recognize many different kinds of attacks and how to stop them. They learn how online security protects a business, but also their own private information. It's the best way to understand how cybersecurity is part of everyone's responsibility.
5. **What is simulated phishing?** *Simulated phishing* is when a cybersecurity training program sends an email to mimic current phishing attacks to see how people respond to email attacks.
6. **What kinds of simulated phishing are there?** An awareness training program has access to thousands of simulated emails. From free donuts, to banking information and emails that can be customized to look like they come from a trusted friend. Simulated emails can even be sent by level of difficulty and ease of recognition.
7. **What happens if I "click" on a simulated email?** You will be redirected to a landing page that says you clicked on a phishing email and then get a list of helpful hints so you can avoid clicking in the future.

8. **What are the most common types of attack?** Email phishing attacks, a targeted attack ("spear phishing"), CEO Fraud, phone calls ("vishing") and texting ("smishing").
9. **What is domain spoofing?** *Domain spoofing*, a common form of phishing, is when an attacker appears to use a company's domain to impersonate a company or one of its employees. This can be done by sending emails with false domain names which appear legitimate, or by setting up websites with slightly different characters.
10. **How do they get my information?** Hackers steal information from places it is stored. They use phishing by sending an email that looks legitimate and with one click, sends the recipient to a fake website and has them enter credentials to "verify" information, which is then stolen.
11. **Wouldn't I know if I have been phished?** Not necessarily! Hackers are tricky. They create emails with a sense of urgency from familiar brands you trust and recognize. It could be your Amazon order isn't delivered. Your boss needs you to wire money. Or even your escrow has closed. It can be hard to spot the fake.
12. **What is a human firewall?** A *human firewall* is someone who follows best practices to prevent as well as report any data breaches or suspicious activity. The more employees you have committed to being a part of the firewall, the stronger it gets.