My Dad works in IT so he is perfect for Case Project 1-1. Back in 2019, his department experienced a spear phishing attempt that managed to successfully deploy a worm.

It all started with a single infected email. From that fake email, the malware struck. Somebody opened a link that brought them to a website that transmitted instructions back to the worm that forced the computer to send out more infected emails to other computers throughout the network.

Because it was now an internal email, it managed to fool more and more people. This worm ran rampant through the network until their Security Operations group blocked the website the worm was getting its instructions from.

If they had found the website before the worm had even been sent, security could have preemptively blocked the website. Additional training could have also prevented this from happening. However, there is only so much training can do as even security professionals can sometimes not pay enough attention to details. Unfortunately the computers were not fixable and so they were all wiped and replaced.