# Student Handout: Stop the Cyberattacks!

Examine the cyberattacks below. For each type of cyberattack, find at least one type of prevention from the next page that will outwit the bad actors.

| Type of Cyberattack | Your Selection of Prevention(s) and Your Reasoning |
|---|---|
| We protect all of our accounts with passwords at Company X—but that's not enough. Bad actors could come after our company Intranet, corporate accounts, and even our email with a brute force attack. They'll enter (and enter and enter) as many common passwords as they can, as fast as possible. If they get lucky, bingo! One of the passwords unlocks a key account, and they're in. Now they have access to our systems and data. Goodbye safe networks and hello headaches...<br>**Attack: Brute Force** | |
| Company X holds tons of private data—exactly what hackers love to steal. Trojans could be a serious threat to our network. This sneaky malware shows up looking like a safe program and could trick any Company X employee into downloading it. Once someone hits that launch button, watch out! The Trojan can open the door for bad actors to steal data and take control of computers (or even the whole network). Trojans can hide themselves or other malware deep in the network, and that can make them really tough to remove. We can't let this happen on our watch!<br>**Attack: Trojan** | |
| Company X employees visit tons of websites every day. Usually, that's okay (plus it's a great way to order lunch). But if someone visits a compromised website, bad news: we could get a drive-by attack! Bad actors hide malware secretly in the code of compromised sites, waiting to snag unsuspecting users in their trap. The malware latches right on to a user's computer, no permission needed, and bam! Attack! Potential vulnerabilities in our network or software are all targets. Now the hackers can access our systems, steal data, damage networks, or even download more malware! We could be in trouble...<br>**Attack: Drive-by** | |
| Just like worms in the earth, computer worms can burrow deep in our systems! This malware can creep from computer to computer, all by itself. The worm creates more and more and more worms—no hacker control or computer program necessary. Just the worm, doing its worst—and the worm is a real troublemaker. It can delete Company X files, change or steal data, spread more malware, or even install a secret backdoor for bad actors to get in later. Because it copies itself over and over again, the worm can really mess up our network too. It can take over our hard drive space and our bandwidth. Let's not let it overwhelm the whole network!<br>**Attack: Worm** | |

| Type of Cyberattack | Your Selection of Prevention(s) and Your Reasoning |
|---|---|
| Think twice: phishing emails look real, but they are a dangerous scam. Phishers pretend to be our partners, or even our coworkers at Company X, all to trick us! They create fake emails that look like our own messages or build sneaky sites to look just like the ones we trust. It's all bait to lure Company X employees into sharing usernames, email passwords, company Intranet access, or even corporate financial accounts and other valuable information. These cybercriminals also sneak malware into email attachments or site code to hack into our systems and steal our data. Let's keep the scammers out!<br>**Attack: Phishing** | |
| Bad news bots! DDoS attacks can sabotage sites in a flash. Whenever a user visits the Company X site, their computer sends us requests for information. Normally, those requests are pretty easy: for example, they might want to see a list of our products or our company's contact information. But DDoS attacks use bots to batter our site! These virtual robot computers complete basic tasks much faster than a person, and they send thousands of requests all at once. It could be enough to shut us down—we have to keep our site from crashing!<br>**Attack: Distributed Denial of Service (DDoS)** | |
| Watch out for macros, the little bits of code that can cause big problems. Macros are meant to be good: they help programs complete tasks in Microsoft Office. But malicious macros hide in innocent-looking attachments. A Company X employee just has to open a Word document or Excel spreadsheet, and the malicious macro is FREEEE! It automatically deploys the malware it carries, and the program starts working to steal all kinds of information. Employees' data, browsing history, webcam files, passwords, you name it: it's a great way for a hacker to get into our system and steal what they want. Keep them out.<br>**Attack: Malicious Macros** | |
| At Company X, we have lots of important records and customer information. Ransomware can make it a huge mess! This malware hijacks our whole network and scrambles our data to make it useless—until we pay up, anyway. The hackers hold the keys to fixing our files, and they have demands. Usually, they want a lot of money, and they'll spread bad news to the press or our customers if we don't give up the cash. Some ransomware will even delete our data forever! Many types of attacks can spread ransomware—we always have to be ready.<br>**Attack: Ransomware** | |