Cyberattack Prevention Strategies

Rate Limiting Request, request, request! RE-lax: we'll just add rate limiting to the Company X website. If we start to get more requests than the site can handle all at once, rate limiting automatically helps us ignore most of them before the site gets overwhelmed. We can always turn it off when we know the website is safe, too. See ya later, attackers!	**Good Password Hygiene** Let's polish up those passwords! If we require Company X employees to change their passwords regularly, it will make their accounts harder to crack. New and different passwords for every account, passwords with a certain number of characters or combinations of letters, numbers, and symbols, and tough-to-guess passphrases all add up to squeaky clean password hygiene. Forget it, attackers!
Maintaining Backups of Data Keep that data up to date and backed up! At Company X, our data is so important. We just can't afford to lose it. If we safely store up-to-date copies of critical data in secure locations (and even offline), we can always count on our backups in case of an emergency or attack. If anything happens to our primary data, boom! We'll be able to restore what we need from the backup copies. Even when hackers come for our data, they'll have no luck: the backups will keep us open for business.	**Disabling Macros** Sorry, macros, you're done. Macros can be useful, but it's just not worth the risk. They can provide a pathway right into the Company X network—it's like giving bad actors a free pass into our systems! If we turn them off and make sure our users can't turn them back on, our system stays safe from malicious macros and their hidden malware. It's still okay if some of the team needs to use good macros—we can choose to limit them and only allow macros with signed digital certificates to make sure they're good ones.
Captchas Good for people, bad for bots: Captchas are simple puzzles for a human to solve, but they're too tough for bots to work out. Think of transcribing a short string of letters or picking particular pictures out of a lineup. If we add a Captcha to the Company X site, we can teach our website not to respond or share information unless a user solves the puzzle. Only real people are welcome to enter the site. Bots, you're out!	**Firewall Blacklist** Is that website really what it looks like? Hackers have a bad habit of hijacking websites to hide malware or building whole new websites and disguising them as safe places when they're not. Looks like we'll have to build some firewalls. If we add a firewall to the Company X network, we'll restrict user access to and from certain websites or types of websites. It'll prevent our employees from accidentally getting stuck with malware, and there's an extra bonus: it stops traffic from hackers trying to break in, too!
Restricting App Downloads Do you know this app? Sometimes what looks like a real computer program or application is really malware in disguise! We don't want that malware on our network. If we restrict app downloads, we can help keep suspicious apps far away from Company X. From now on, employees will only be allowed to download company-approved programs or applications from official app stores. App-solutely better protection.	**Network Segmentation** The Company X network keeps us all connected—but we can't make it too easy for bad actors to connect with everything, too! Let's segment our network. That way, our devices can still talk to each other, but it will be much harder for hackers to hop from one area of the network to another. We'll need to put up walls between different parts of the network: virtual partitions like firewalls work, and so do the physical boundaries of separate buildings.
Two-Factor Authentication (2FA) It's time to require two-factor authentication. 2FA adds a step to accessing an account: instead of just a username and password to log in, two-factor authentication also requires entering a code from an email or text message. Even if a hacker steals an account username and password, they can't get in without the code! Company X employees will need the code to access tools like email or company Intranet, too. From now on, we'll need a backup email or cell phone for all of our accounts—that way, Company X users can access the code and authenticate themselves on new devices or unrecognized computers.	**Installing Updates and Patches** Patch that! Nobody's product is perfect, so software companies work constantly to fix problems in their programs and keep things running smoothly. Sometimes these problems result in vulnerabilities, aka easy places for bad actors to break in. Whenever a company releases a new update or a patch for a vulnerability, our team has to be on the job! We need to install the updates quickly across all the devices in our company because hackers are always on the prowl. They'll be searching for unprotected devices to target, and we can't let them find any here.