According to the information presented, Natalya was the victim of a phishing attempt in which the attacker edited the email to appear to be from the IT department, but it was delivered by a hostile actor. The email's purpose was to persuade Natalya to download and install malware disguised as an update, enabling the attacker remote access to her system.

To avoid and identify such attacks, organizations must have strong security measures in place. Employees who get frequent cybersecurity awareness training can help reduce the likelihood of successful phishing attacks, safeguarding both the company and its employees.

Next, to avoid further harm, the first step in this situation would be to disconnect Natalya's computer from the network. If I were a cybersecurity professional, I would start the incident response process right once by assessing the kind and breadth of the attack, as well as whether any other systems were hacked. Natalya should then change all her passwords and keep an eye on her other online accounts for any unusual activity. I'd also advise her to alert me if she observes any unusual computer activity or changes to her files or settings.

Finally, to avoid a repetition of this situation, it is vital to educate employees about phishing efforts and how to identify them. Additionally, the company should have extensive security procedures in place to identify and prevent unauthorized access. Spam filters, email authentication methods, and endpoint protection software can all help to prevent these types of attacks. Regular cybersecurity awareness training and testing may help employees emphasize the importance of cybersecurity and reduce the likelihood of successful phishing efforts. Phishing attacks are prevalent, and employees must be informed of the risks and how to spot them.