

Recognizing and Avoiding Scams

Mary struggled to remember passwords, so she decided to use the same combination of four letters and four numbers for everything. She knew it was a risk, but didn't really care.

One morning, Mary arrived early to work to check her e-mail. At the very top of the email list was one sent to her by her boss. The name was spelled wrong, but she shrugged it off as a typo.

Her heart started racing—it was her boss urging her to change her password as quickly as possible, “There’s been a breach in the company and all passwords were leaked to an outside source.” they said. “Source” was spelled wrong, but again, just a typo. Mary hurriedly followed the email’s instructions and hit the link, “ClickHere” found at the bottom of the email. She entered her workplace username and password and continued about her day as normal.

The next day Mary received another email. This one from HR stated that a company wide email scam was reported to have collected usernames and passwords from multiple employees. The email ended with a friendly reminder: “Please stay vigilant in checking the validity of your emails and if you have experienced anything fishy, go straight to HR.”

Mary was embarrassed but spoke to HR about what had happened. Debbie from HR explained to her that since the Hacker had Mary’s login information, it was best to change her current work username and password. Debbie also encouraged Mary to change any other existing passwords to accounts outside of work so long as they were similar to those given to those entered in the scam email. Mary had her work cut out for her. Since Mary used the same password for everything, she had to set apart time outside of work to remember all the websites and accounts that required a password and change them to something different.

1. What type of scam did Mary fall victim to?

2. What’s one red flag that the email was a scam?

3. What type of scam did Mary fall victim to?
