# NOW SHOWING
RECOGNIZING AND REPORTING PHISHING

The reviews are in: phishing is popular among hackers and can be catastrophic for organizations. Phishing makes up 44% of social engineering incidents, and **98% of phishing incidents are via email**. But it isn't enough to simply know that phishing emails are out there; you also need to be able to recognize and report them.

Lights. Camera. Hack-tion

Let's preview some of the big hacker heists that hit the screens this year
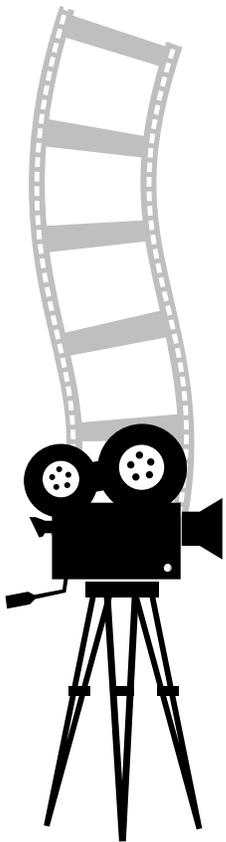
Urgent message
- An urgent phishing email is designed to get you to act fast. It might tell you that your account was hacked or will be deactivated — click here to restore it! Fear makes people do things without thinking, so slow down!

Login or password message
- Another type of phishing email asks you to verify your account by logging into a (fake) webpage or updating your credentials. These emails can collect your username and password, giving a hacker instant access to your account.

Corporate communications
- According to the 2023 Verizon Data Breach Report, business email compromise attacks have almost doubled across their entire incident dataset. We've seen this firsthand with our customers. Hackers use corporate communications and emails from stakeholders such as HR or leadership, which tend to have the highest click rate. An internal message phishing email might ask you to click on a link to read and sign a policy, read a document about a company-wide update or even hand over sensitive information.

Reward or free gift message
- Receive an invite to a free movie premiere? Be on high alert! Free things are enticing, but they can also be dangerous. Hackers are trying to bait you into clicking a malicious link.

If you think you've encountered a phishing email: Follow company procedures for reporting. Once the right people are notified, they can help you determine if it's a phishing email. Whatever you do, do not click on any links, reply to the email or send it to anyone else!

INFOSEC

SECURE YOUR SCREEN

E-TECH