TIMELINE OF A PHISH

A SPEAR PHISHING ATTACK DOES NOT JUST HAPPEN OVERNIGHT.

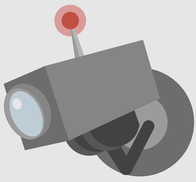
SOCIAL ENGINEERS CAN SPEND **MONTHS** PLANNING AN ATTACK, AND IT CAN TAKE OUR ORGANIZATION **MONTHS** TO UNDO THE EFFECTS OF A DATA BREACH.

SEE BELOW, STEP BY STEP, HOW AN DATA ENTRY STYLE ATTACK UNFOLDS

Social engineers spend a great deal of time researching their targets. With free or paid resources, one search is all it takes to learn all about you.

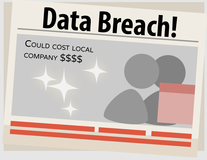
With knowledge of your personal and professional interests, a spear phisher sends a highly personalized email with a weaponized link.

The link takes you to a landing page, where you are prompted for login credentials. “Logging in” gives the spear phisher access to your account.



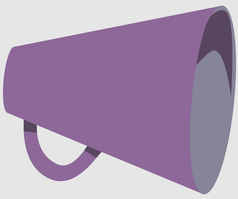
With full access to your private account, the spear phisher begins digging for private information or a way to access our network.

If our network is breached, it can take an avergae of 24 days and 591,000 USD to fix. [1]



It can take even longer to fix the damage done to our organizations reputation by a data breach.

Rather than ignoring a suspcious email, you can alert our organization by reporting an email rather than ignoring it.



KEEP AN EYE OUT FOR THE COMMON WARNING SIGNS OF A PHISH:

UNKNOWN **SENDER**

GRAMMATICAL **ERRORS**

PLAYS ON YOUR **EMOTIONS**

REMEMBER
A LEGITIMATE ORGANIZATION WILL NEVER SEND AN UNSOLICITED REQUEST FOR **YOUR PASSWORD.**

IF AN EMAIL SEEMS SUSPICIOUS, DON’T TAKE A CHANCE. REPORT IT TO KEEP OUR ORGANIZATION SAFE.

COFENSE

SOURCES
1. http://media.scmagazine.com/documents/54/2013_us_ccc_report_final_6-1_13455.pdf