

CLICK THINKING

Quick insights for protecting yourself and your company from online threats

I N F O G R A P H I C



BUT THE GOAL IS

PRIME DIRECTIVE:
TRICK, FOOL, DECEIVE



ALWAYS THE SAME



MAY INCLUDE SPELLING MISTAKES OR GRAMMATICAL ERRORS

EMAIL DEMANDS IMMEDIATE ATTENTION OR THREATENS DIRE CONSEQUENCES FOR NOT ACTING

INCLUDES AN OFFER THAT SEEMS TOO GOOD TO BE TRUE

COMES FROM AN UNLIKELY SENDER

REQUESTS SENSITIVE INFORMATION LIKE ACCOUNT NUMBERS OR PASSWORDS

ASKS YOU TO VERIFY ACCOUNT INFORMATION

IS ADDRESSED TO 'UNDISCLOSED RECIPIENTS' OR HAS NO ADDRESSEE WHATSOEVER

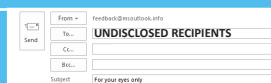
JUST FEELS OFF

Important account alert!
Click link immediately to have no funds insufficient!!!

Hello, this is your Board Chairman. Please send our bank log-in credentials to the link below immediately.

Unclaimed property in your name worth \$1.4 million awaits your claim. Click now!

Please send network passwords to our remote office so they can access the system asap!



LEARN THE LANGUAGE OF PHISHING SO YOU CAN SPOT THE SCAMS

NEVER CLICK A LINK FROM A SUSPICIOUS EMAIL!

Hey there! It's me again, hoping to trick you into opening the email I just sent your way.

Perhaps you've seen it? The subject line was a real attention grabber. And if you opened it, you might have seen an offer for something that sounded too good to be true.

This time it was a free time share for a month! Next time, I might pretend to be your CEO and demand you send our tax ID numbers to our overseas partners right away.

Of course, none of these promises or demands are real. But that's how phishers like me work.

So go ahead and click that link—if you want to make my day!

