Phish Phinder
Tell-Tale signs of a (potentially) successful Email Phishing Scam

Hackers use Phishing Emails to obtain your:
- Usernames
- Passwords
- Credit Card #

All it takes is for you to take the bait by:
- Opening an attachment
- Clicking a malicious link
- Entering sensitive information

Anatomy of a Phishing Email
Look for any of the following suspicious elements when opening your next email.

- Is the subject relevant to my relationship with the sender?
- Is the sender's email address correct?
- Is the email directed at undisclosed-recipients?
- Was it sent to several addresses?
- Is this a normal time/date for this sender to have emailed you?
- Is the subject relevant to my relationship with the sender?
- Is the issue really as urgent as the sender is implying?

Red Flags
- Is the content relevant to your relationship with the sender?
- Is the name of the sender relevant to my relationship with the sender?
- Is the email directed at undisclosed-recipients?
- Was it sent to several addresses?
- Is this a normal time/date for this sender to have emailed you?

Don't Take the Bait
1 in 10 Phishing Emails Succeed

Remember:
- A little scrutiny goes a long way
- Be aware of the warning signs and don’t ignore them
- If it doesn’t look right, it probably isn’t.
- Take a closer look before taking action
- Even the most savvy can still get caught.

Keep your anti-spam or anti-virus software up to date.
Secure your network traffic to mitigate phishing risk at your company!

© Avast Software s.r.o. 2021