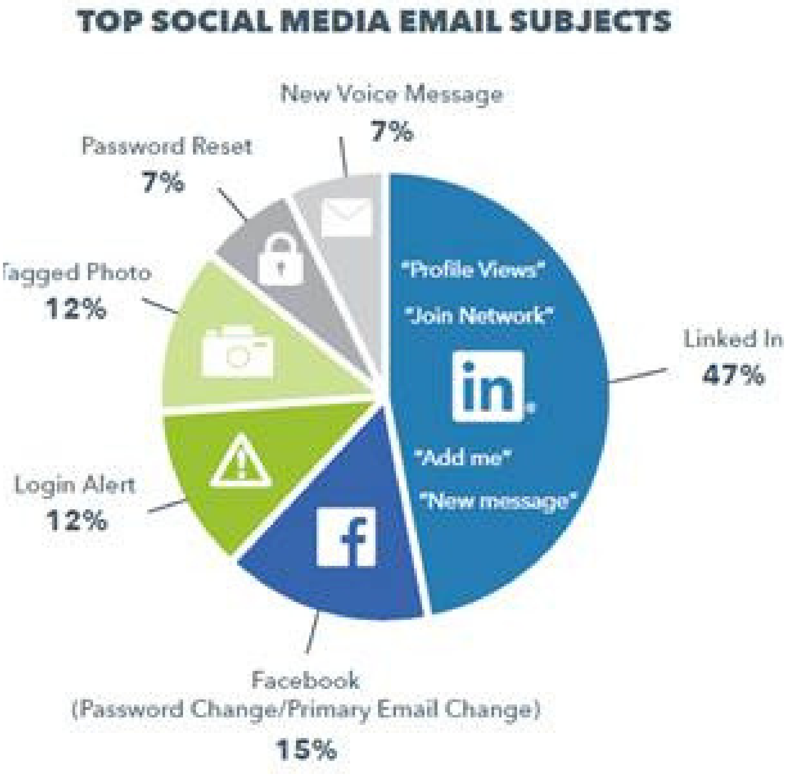
PHISHING SCAMS #1 WAY THIEVES STEAL FROM BUSINESSES

According to Mimecast's State of Email Security 2018 found 90% of organizations have seen an increase in the volume of phishing attacks. 49% of organizations admit that their staff and finance teams are not knowledgeable to identify and stop a phishing email that is seeking to steal money or confidential information. The Mimecast study found that this lack of awareness resulted in 31% of senior employees sending sensitive information or money to the wrong person last year. Phishing is the most common means that bad individuals use to steal financial and confidential personal information from businesses. Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message.

Certain types of messages sail through personal security defenses because they play into the human psyche. Whether it is wanting to be popular or recognized, these types of emails make a person feel important or alarmed. These attacks are effective in that they try to get the target to either avoid a negative consequence or gain something of value. Also, a single-stage phish is easier to accomplish than a cyber-attack on a company's server because it exploits an immediate psychological "knee-jerk" impulse.

Top 10 PHISHING Email Subjects used to obtain your financial and confidential personal information sent to employees.



- A delivery attempt was made: 21%
- Chang of Password is required immediately: 20%
- W-2 Update: 13%
- Company policy update for Fraternization: 10%
- UPS Label delivery 1ZB3313TNY0001602: 10%
- Revised Vacation & Sick Time Policy: 8%
- Staff Review: 7%
- Urgent press release to all employees: 5%
- Deactivation of your Email is in process: 4%
- Please Read: Important news for HR: 2%

Email is an effective way to phish users when disguised as a legitimate email. These methods allow attackers to craft and distribute enticing material for both ransom (general phish) and targeted (spear phish) means, leveraging multiple psychological triggers. Train your staff to be cautious when receiving unusual or unexpected emails and not to provide confidential information, passwords, or financial information without confirming the legitimacy of the request or sender if there is any doubt.

Financial losses resulting from phishing emails are often not covered by basic Crime or Property insurance policies but may be covered by a separate Cyber Liability policy. So check your policies for what is or is not covered before you and your business becomes a victim.