INKY

Phishing Prevention Checklist

Human error continues to be the biggest access point to exposing company data to cyber attacks.* Phishing, BEC, and email account takeover cost businesses hundreds of thousands of dollars annually. So how can you help your employees, or your first line of defense, limit the number of successful phishing attempts?

This checklist will help you to build the best defense possible against phishing attempts.

Ongoing Employee Training

- Do you know and trust the sender?
- Is the request unusual?
- Does the senders email seem out of place?
- Does the email lack personalization?
- Grammar issues
- Threatening
- Strange attachments

Never share personal information.

- Social Security Number
- Personal contact information
- Passwords
- Financial information

Does the email contain urgency?

- Deal ending
- By this time or miss out

Share examples

When you have incidents happen, anonymize them and use them to show employees what it looks like in the real world.

Install INKY Phish Fence

INKY's powerful computer vision makes identifying a malicious email easier. By leveraging machine learning and AI to identify if key features of the email are fishy. The color-coded banner quickly alerts employees that something if off with these emails and warrants deeper investigation and provides a route to remediation.

www.inky.com