Catch the “Phish” – Beware of Common Phishing Attacks

Phishing attacks have become a top priority for all kinds of organizations to be prepared for. Education is key – and so is knowing about the most common types of phishing attacks and how to identify them.

**DECEPTIVE PHISHING**
- Biggest fish in the sea
- Sends email from trusted sender
- Steals information by imitating a legitimate provider
- Inspect URLs carefully
- Check for legitimate redirections
- Check: generic salutations, grammar mistakes, spelling errors

**SPEAR PHISHING**
- At home on social media sites
- Sends email from recognized sender and uses personalized information
- Cybersecurity User Awareness Trainings
- Limit sharing personal information
- Invest in automated solutions to analyze emails

**CEO FRAUD**
- Keen on executives
- Aims on getting authorizations for financial transfers
- Cybersecurity User Awareness Training for executives
- Setting up Multi-Factor Authentication (MFA) for financial transactions

**VISHING**
- Loves hanging on the phone
- Mimics known entities to steal sensitive data
- Avoid taking calls from unknown numbers
- Never share sensitive / personal information via phone
- If in doubt, call back entity on a known number and verify previous call

**SMISHING**
- Loves SMS and text messages
- Mimics known entities to steal sensitive data
- If in doubt, call back entity on a known number and verify that the message was sent on purpose

**PHARMING**
- Changes IP address associated with a website name
- Redirects to a malicious website
- Only use https protected sites
- Use anti-virus software / security settings and regularly update

Source: tripwire