Don't get hooked Stop and think before opening any attachments, especially from an unknown source, as they can be malicious. Double check if it is a legitimate email. If this is your corporate email, notify your IT staff. Do not reveal personal information Never give up any personal information from an unsolicited email. Phishing emails will attempt to steal your personal data/information by pretending to be someone else. The letterhead might look official, but a legitimate organization will never email you to ask for your password or any other sensitive information. Legitimate organizations do not generally ask you to verify username and password, except for initial setup. If things look ‘phishy’, verify the sender through a different medium, for example by calling and confirming.

Educate your users Phishing relies on human errors. Training the users or your employees regularly is one of the most effective ways to eliminate threats. Organizations must conduct training and awareness workshops to make sure the employees are aware of the do’s and don’ts, and ways they can detect and prevent phishing attacks.

Check for grammar/spelling errors Spelling errors are often used in English, or they are not too bothered about spelling and grammatical mistakes. Check for poor spelling, typos/punctuation errors in the email, which could be a tell-tale sign of the fact that the sender is a scammer. Check for the salutation and closing off too, as they may be vague or worded incorrectly or oddly.

Check website URL Check the URL of the website to ensure it is not the real website. Phish emails that use HTTPS rather than HTTP will always force the user to hovering over them than before you click. The site might look legitimate, but the actual website URL could be fake. If you think you need to visit a website, type out its address in the search bar.

Up-to-date security measures Install the latest patches and updates to protect against vulnerabilities and security issues. Detect phishing activity, responding effectively and neutralizing the threat takes times and skill. Ensure your organization has the right tools and technologies, without which the intrusion could go unnoticed for months. Put anti-phishing protection measures at every point in your business.

Be wary of emails asking you act urgently Be cautious if an email uses urgent language or makes you offers and promises of rewards that are too good to be true.

Number of unique phishing websites detected in Dec: 45,794
Number of unique phishing email reports (campaigns) received by APWG from consumers in Dec: 87,386


Stop your business from taking the bait with the following tips

Think before you click Never click on links in emails claiming to be from a legitimate business or organization. Many of these attacks download trojan horse virus on the computer when the link in the email is clicked on. Check the link and make sure the link is from a reputable source before clicking on it.

Write to us at: business@happiestminds.com

About Happiest Minds Technologies
Happiest Minds, the Mindful IT Company, applies agile methodologies to enable digital transformation for enterprises and technology providers by delivering seamless customer experience, business efficiency and actionable insights. We leverage a spectrum of disruptive technologies such as: Big Data Analytics, AI & Cognitive Computing, Internet of Things, Cloud, Security, SDN-NFV, RPA, Blockchain, etc. Positioned as “Born Digital . Born Agile”, our capabilities spans across product engineering, digital business solutions, infrastructure management and security services. We deliver these services across industry sectors such as retail, consumer packaged goods, edutech, e-commerce, banking, insurance, hi-tech, engineering R&D, manufacturing, automotive and travel/transportation/hospitality.

Headquartered in Bangalore, India; Happiest Minds has operations in the U.S., UK, The Netherlands, Australia and Middle East.