TO CLICK OR NOT TO CLICK, THAT IS THE QUESTION

How to protect users from phishing in a "click first, ask later" culture

95% of all attacks on enterprise networks are the result of successful spearphishing.[1]

15–20% of a worker's web sessions (i.e., opening a browser) are initiated by clicking a link in an email.[2]

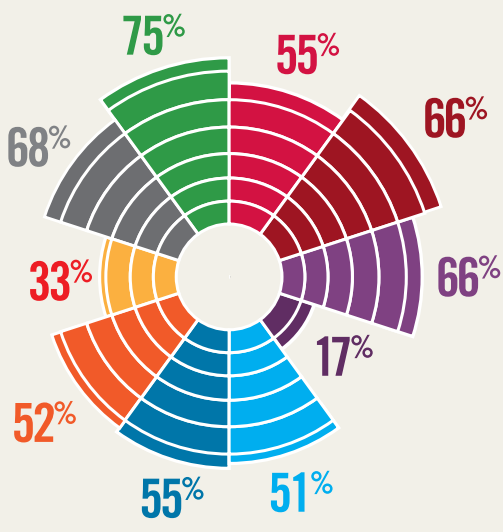
Email-based attacks accounted for 79% of social breaches in 2012 (a category which also includes SMS, websites, and documents).[3]

78% of active email users in the US will also access their email through a mobile client by 2017.[4]

But from a mobile device, it's difficult for users to hover over links to determine whether the link is safe or not before they click on it.

PEOPLE FEEL COMFORTABLE GETTING EMAIL ANYWHERE – ON ANY DEVICE

Around the world, more people are accessing email from a smartphone than ever before.[5]



- AUSTRALIA
- BRAZIL
- CHINA
- INDIA
- ITALY
- RUSSIA
- SOUTH KOREA
- TURKEY
- UNITED KINGDOM
- UNITED STATES

92% of employees trust the security of their company's email system and feel their email is safe.[2]

49% of those surveyed have conducted company business on a public Wi-Fi network,

BUT

only 10% feel confident in the security of public Wi-Fi networks.[2]

80% of security professionals said laptops and mobile devices were a significant risk vector,

BUT

only 13% enforced stricter standards on personally owned devices.[6]

To prevent phishing attacks from succeeding, every employee has to be covered on every device. Personal devices and public networks can no longer be left out of the security policy.

BETTER EMAIL SECURITY IS NEEDED TO PROTECT AGAINST DELAYED MALWARE IN LINKS

Smart security means fewer opportunities for malicious attacks to compromise your network.

With proactive zero-day malware protection and safe previews of upcoming pages, you can expose phishing attacks before they happen.

WANT TO LEARN MORE? >> WATCH THE VIDEO.

Visit us at **McAfee.com/emailsecurity**
and don't forget to follow us on Twitter **@McAfeeBusiness**

SOURCES:
1. Network World - http://www.networkworld.com/news/2013/030613-spear-phishing-267409.html
2. Repass & Partners, Inc. – Nationwide online survey, 2013
3. Verizon - http://www.verizonenterprise.com/DBIR/2013/
4. Forrester - http://blogs.forrester.com/jitender_miglani/12-10-18-78_of_us_email_users_will_also_access_their_emails_via_mobile_by_2017
5. Email Monday - http://www.emailmonday.com/mobile-email-usage-statistics
6. Ponemon - http://www.ponemon.org/local/upload/file/2013%20State%20of%20Endpoint%20Security%20WP_FINAL4.pdf

McAfee®
An Intel Company