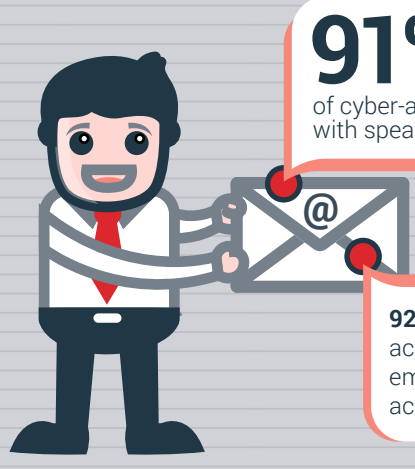
THE STORY OF A PHISH

MEET TROY.

Troy works for a local utility company.

40% of cyber-attacks in 2012 were targeted at the energy industry

HE STARTS EVERY MORNING BY CHECKING HIS EMAIL.



91% of cyber-attacks begin with spear phishing

929 million business email accounts, **100 billion** business emails sent/received each day, accounting for **55%** of all emails

At 10:00 am, Troy walks to the cafeteria for his daily latte & bagel.

WHILE HE'S WAITING FOR HIS BEVERAGE, HE CHECKS FACEBOOK ON HIS CELL PHONE.

Hackers access credentials and research social media profiles to gain intelligence about people they're targeting. Their goal is to build highly personalized "lures" that are likely to be opened.

1.15 BILLION people use Facebook

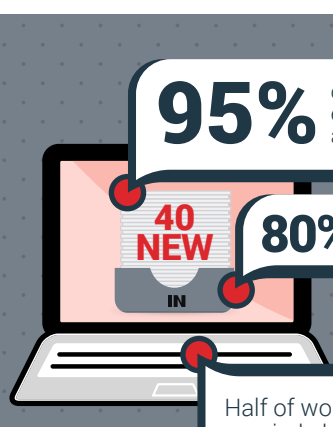
Facebook users share **2.5 BILLION** pieces of content per day

25% of Facebook users do not use privacy settings

20% of social media users set their profile to completely public

BACK AT HIS DESK, TROY DISCOVERS HE AMASSED 40 WORK EMAILS WHILE HE WAS AWAY.

He quickly runs through them, not paying particular attention to where he's clicking.



95% of state-affiliated espionage attacks employed phishing as a means of establishing a foothold in their intended victims' systems.

80% of breaches exploited normal users not system admins

Half of workers are more worried about being phished at home than at work

One email catches his eye. It appears the company is holding a series of training sessions to help employees avoid phishing attacks.

HE DELETES THE EMAIL. HE'S NOT CONCERNED, AS HIS COMPUTER HAS ANTI-VIRUS AND ANTI-SPAM SOFTWARE.

58% of users will click on a phishing link prior to training, number can be reduced to <10% after 12 months of training

100,000 new malware samples created daily

ANTI-SPAM IS NOT 100% EFFECTIVE. Not even anti-spam vendors claim 100% effectiveness

ONLY 61% OF PHISHING LINKS ARE CORRECTLY IDENTIFIED AND BLOCKED BY CHROME, the highest percentage among leading browsers

HE GETS A TEXT FROM HIS WIFE JILL, REMINDING HIM ABOUT DINNER WITH THE NEIGHBORS THAT NIGHT.

Jill works as an HR manager for a local technology company.

Manufacturing, Services and Technology industries: **91% of attacks took hours or less to perpetrate and 62% of those attacks took months—or even years- to detect**

A calendar reminder pops up on Troy's screen. It's time for the weekly team meeting. He grabs his cell phone and notebook and heads to the conference room.

WHILE IN THE MEETING, TROY TUNES OUT & CHECKS TWITTER ON HIS CELL. HE ALSO CHECKS HIS WORK EMAIL TO FEEL PRODUCTIVE.

500 MILLION tweets sent per day

88% of Twitter accounts are unprotected

Mobile email market projected to double by 2017

HE CLICKS ON AN EMAIL THAT APPEARS TO BE FROM A REPUTABLE FINANCIAL ORGANIZATION.

Troy has now unknowingly fallen victim to a phishing scam.

Financial themes continue to be the most frequently spoofed subject matter, with **61.6 PERCENT** of phishing scams containing this theme compared to other markets:

INFORMATION SERVICES 33.8%
RETAIL 5.2%
COMPUTER SOFTWARE .9%
COMMUNICATIONS .5%

THE AFTERMATH

COST OF A SUCCESSFUL PHISHING ATTACK:

Average annual cost of cyber-crime
$8,900,000 (2012)
$11,600,000 (2013)

Cost per compromised record
$222

EXAMPLES:

SC Department of Revenue:
$14M, $700K FOR IR COSTS

RSA breach:
$66 MILLION IN 2011

PHISHME

SOURCES

http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-spear-phishing-email-most-favored-apt-attack-bait.pdf
http://media.kaspersky.com/pdf/Kaspersky_Lab_KSN_report_The_Evolution_of_Phishing_Attacks_2011-2013.pdf
http://fuelfix.com/blog/2013/01/14/cyber-attacks-at-energy-facilities-jump-40/
http://www.mcafee.com/us/security-awareness/articles/state-of-malware-2013.aspx
http://www.proofpoint.com/products/protection/anti-spam-effectiveness.php
http://www.ijser.org/researchpaper%5COn-Effectiveness-of-Various-Browsers-in-Phishing-Detection-An-analysis.pdf
http://www.radicati.com/wp/wp-content/uploads/2013/04/Email-Statistics-Report-2013-2017-Executive-Summary.pdf
http://www.pewinternet.org/~/media/Files/Reports/2012/PIP_Privacy_management_on_social_media_sites_022412.pdf
http://www.digitalbuzzblog.com/infographic-social-media-stats-2013/
http://ivn.us/2013/10/02/7-social-media-stats-2013-will-surprise/
http://blog.bufferapp.com/10-surprising-social-media-statistics-that-will-make-you-rethink-your-strategy
http://expandedramblings.com/index.php/march-2013-by-the-numbers-a-few-amazing-twitter-stats/
http://www.beevolve.com/twitter-statistics/
http://www.scnow.com/news/politics/article_69f12c14-395b-11e2-8d70-001a4bcf6878.html
http://www.informationweek.com/attacks/rsa-securid-breach-cost-$66-million/d/d-id/1099232
Websense 2013, Threat Report
http://www.websense.com/assets/reports/websense-2013-threat-report.pdf
Massive-scale phishing attacks loom as new threat, USA Today
http://www.usatoday.com/story/cybertruth/2013/05/08/longlining-phishing-cybersecurity-privacy/2134445/
Ponemon Institute: 2012 Cost of Cyber Crime Study
http://www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6%20.pdf
Ponemon Institute: 2013 Cost of Cyber Crime Study
http://media.scmagazine.com/documents/54/2013_us_ccc_report_final_6-1_13455.pdf
2012 Verizon Data Breach Investigations Report
http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012-ebk_en_xg.pdf
Spear phishing' the main email attachment threat, ComputerWorld UK
http://www.computerworlduk.com/news/security/3413523/spear-phishing-the-main-email-attachment-threat/
Verizon Research Report
http://www.verizonenterprise.com/resources/factsheets/fs_dbir-industries-manufacturing-services-technology-threat-landscape_en_xg.pdf
SYMANTEC INTELLIGENCE REPORT
http://www.symantec.com/content/en/us/enterprise/other_resources/b-intelligence_report_12-2013.en-us.pdf
Cost of a Data Breach: Director of SC Department of Revenue Resigns, Breach Costs Over $14M
http://www.alertboot.com/blog/blogs/endpoint_security/archive/2012/11/27/cost-of-a-data-breach-director-of-sc-department-of-revenue-resigns-breach-costs-over-14m.aspx