Combating Email Fraud

Maitham Al Lawati, CISSP, CISM, CRISC, CCSP, CEH, ISO27001 LI
General Manager – Risk, Compliance & MSS

URS is a member of Registrar of Standards (Holdings) Ltd.

TÜVRheinland®
Precisely Right.

ISO27001:2013

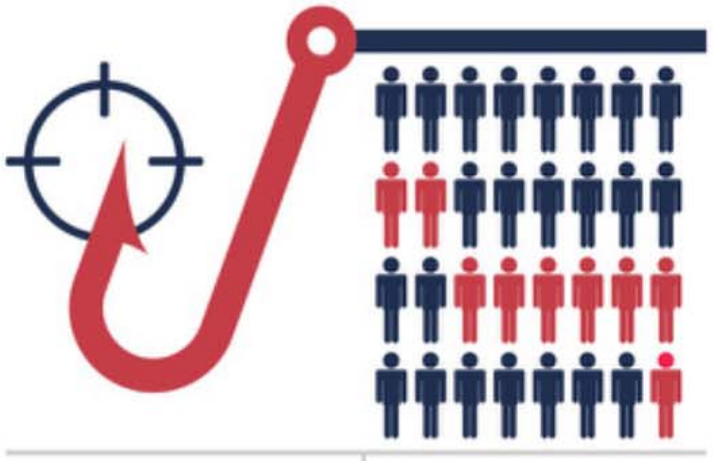
OMAN DATAPARK
MANAGED SECURITY SERVICES

u2

DID YOU KNOW...

JUST ONE CLICK

CAN COMPROMISE YOUR BRAND,
PUT YOUR CUSTOMERS' DATA AT RISK,
AND DESTROY CONSUMER TRUST?



Do you know that the bad guys can send spoofed emails on behalf your domain name and they can be reached to your partners, customers and maybe even to your own staff?

Slide 2

u2 user, 11/4/2017

Organizations Problems with Email

1 Fraud email is sent to customers & business partners

- 100 billion spam messages globally per day
- 2.1 million phishing messages per day
- 73% of data breaches begin with a fraudulent email

2 It is difficult to identify fraudulent email

- Phishing emails have a 70% open rate
- 50% of users to open phishing email will open the URL or attachment

91% of cyber attacks start with phishing[1]


The Telegraph

HOME | NEWS | SP

Money | Consumer affairs

Investing | Property | Bills | Insurance | Pensions | Banking | Tax | A-Z | Financial

Money / Consumer affairs

Another homebuyer loses £67k as solicitors fail to warn of email fraud


SALTED HASH- TOP SECURITY NEWS

About

Fundamental security insight to help you minimize risk and protect your organization

NEWS

Chinese scammers take Mattel to the bank, Phishing them for $3 million

Thieves took advantage of a recent company shakeup and corporate policy regarding payments


May 01, 2017

Facebook and Google confirm falling victim to £77m phishing scam

Back in March, a Lithuanian man was arrested for duping two unnamed multinational internet companies via an email phishing attack.

Google and Facebook have confirmed that they were the two companies that fell victim to the scam costing them $100 million (£77m).

274% increase in phishing[2]

$2.3bn cost of CEO to CFO fraud[3]

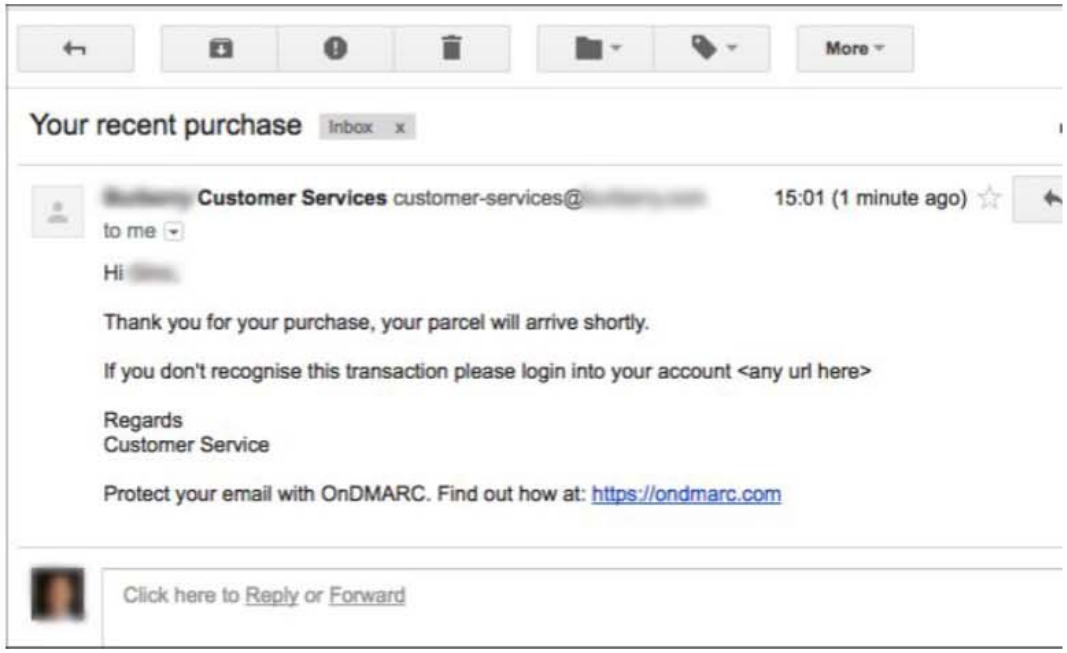
97% cannot correctly identify a phishing email[4]

Impersonation is easy

A gap in the email protocol allows anyone to easily send emails using your domain.

Easily done with everyday tools like telnet.

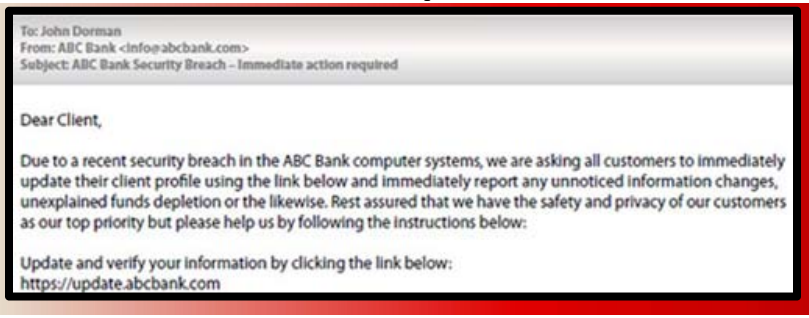
"CEO to CFO scams acounted for $2.3 billion in losses in the past 3 years" - FBI 2016



Fraud Email is the Start of a Data Breach

- 73% of data breaches begin with fraudulent email. The below scenarios are common methods to breach consumers devices or employee's "bring your own devices".

User Credential Compromise


To: John Dorman
From: ABC Bank <info@abcbank.com>
Subject: ABC Bank Security Breach – Immediate action required

Dear Client,

Due to a recent security breach in the ABC Bank computer systems, we are asking all customers to immediately update their client profile using the link below and immediately report any unnoticed information changes, unexplained funds depletion or the likewise. Rest assured that we have the safety and privacy of our customers as our top priority but please help us by following the instructions below:

Update and verify your information by clicking the link below:
https://update.abcbank.com

- **URL to website to capture login credentials**
- **Compromised username & password often reused across websites**

Malware Installation


Xerox Printer <printer@xerox.com>
Bonus Structure
To

Please download the document. It was scanned and sent to you using a Xerox multifunction device.

File Type: pdf
Download: Scanned from a Xerox multi~9.pdf

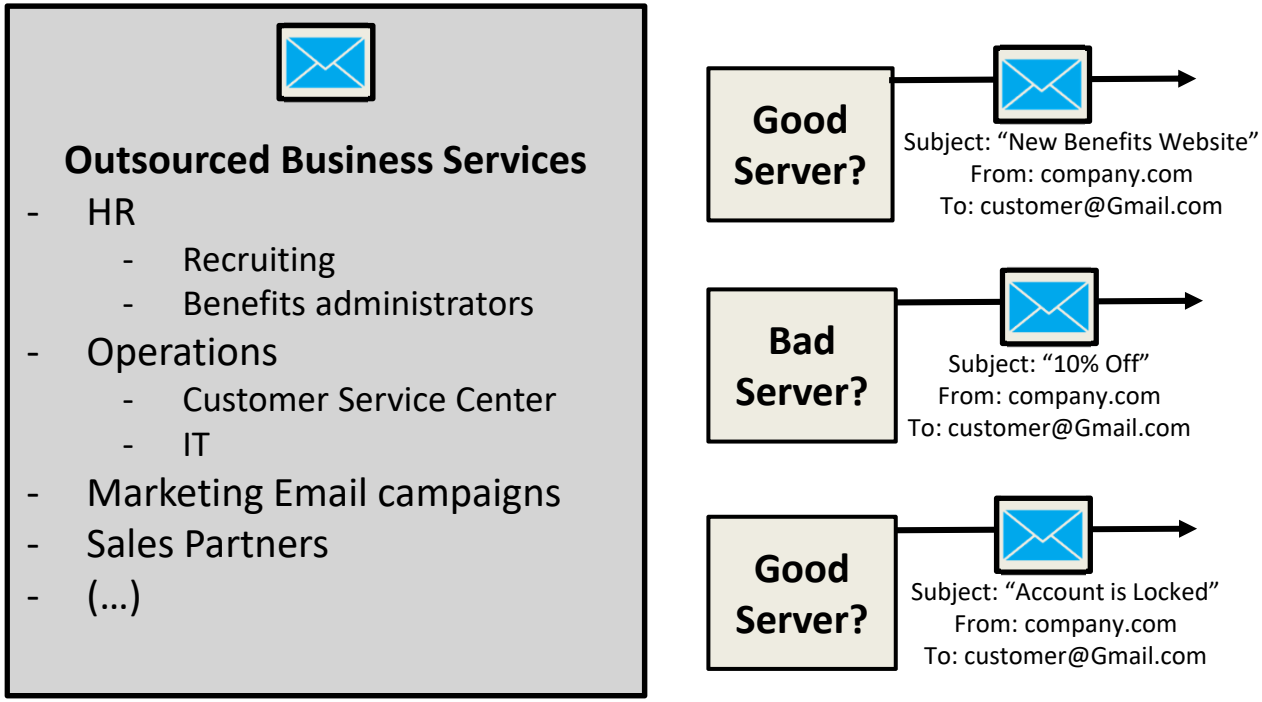
multifunction device Location: machine location not set
Device Name: Xerox2343

- **Email often spoofs YourCompany.com, YourCompamy.com, or other trusted domain**

- Fraud Expenses
- Brand Erosion
- Untrusted Emails

Difficult for Companies to Identify Emailers

- Outsourcing companies send email spoofing FROM:@company.com from their own IP addresses.



The IT needs to distinguish
fraud emails senders vs. outsourced senders.

DMARC

A PROVEN WAY TO MITIGATE RISK

Domain-based Message Authentication, Reporting and Conformance (DMARC)
It's like an identity check for your organization's domain name.

DMARC prevents spammers or phishers from using valid organization names for email fraud

DMARC increases customer **confidence and trust**

It protects the integrity of **your brand**

DMARC Benefits for Financial Services

Gain 24/7/365 Email Spoofing Visibility

Leverage DMARC Authentication to Strengthen Email Security & Brand Protection

Decrease Fraudulent Email Delivery to by Over 99%

Restore Trust with Consumers via email communication

How well does it work?

"Implementing DMARC stopped nearly 25 million attempted attacks on our customers during the 2013 holiday buying season alone"

Michael Adkins, Facebook

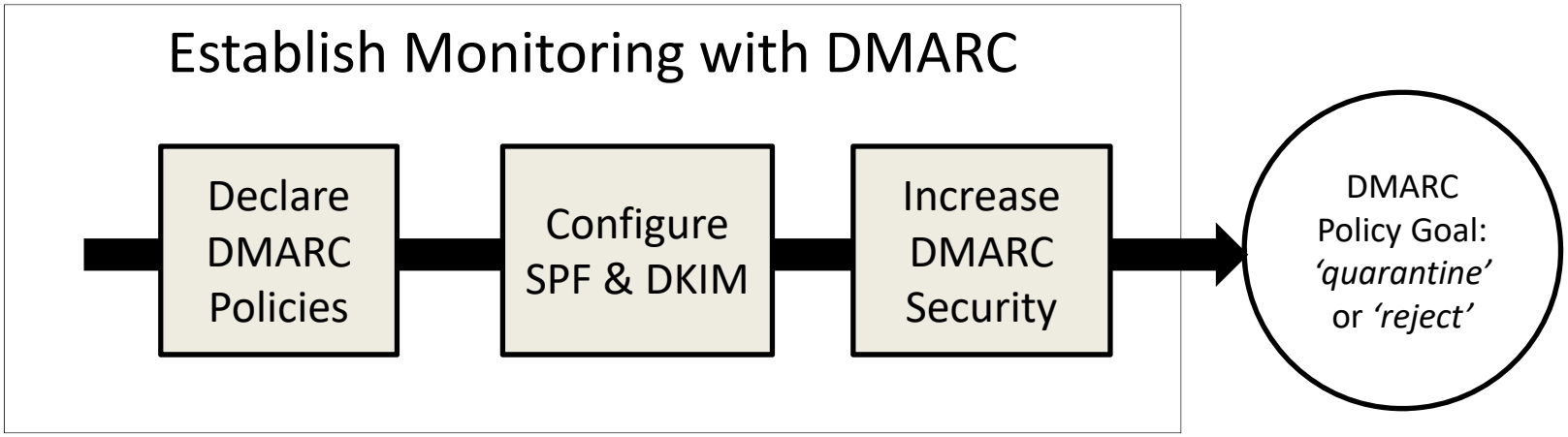
"DMARC protects more than 85% of the people who receive email from Facebook"

Trent Adams, PayPal/Ebay, Chair of DMARC.org

Twitter saw 110 million spoofed emails per day. Once Twitter moved to a DMARC "reject" policy, the number dropped to few thousand within days.

* DMARC.org, http://www.dmarc.org/news/press_release_20140218.html

Summary of DMARC Recommendations



Recommendations

1) Have a DMARC policy goal for each domain and sub-domain
2) Create a DMARC policy on each sub-domain to detour spoofing
3) Predefine the advancement criteria from p=none to p=quarantine to p=reject
4) Ensure DMARC pass rate of 98% - 100% before advancing the DMARC policy
5) Advance all parked domains to p=reject as a final state