The Human Firewall is on fire – Anatomy of an email-based attack.
Cyber Security Today

Defense Arms Race
Threats are constantly evolving!

Data Recovery
Can we recover to the last safe state!

Skills Deficiencies
It’s difficult to attract and retain talent!

Business Disruptions
How do we maintain availability during a disruption!
Email Attacks

~30% of phishing attacks were opened
Median time to first click
91% of attacks start with a phish
66% of malware was installed via malicious email attachments
$5B global scam

Why do attackers rely on email?
Cheap, ubiquitous, global, flexible, anonymous, trusted by users, integral to so many business processes

225B
Emails sent everyday

#1
Office 365 Cloud Service by User Count

6.3B
Email Mailboxes in 2017, growing to 7.7B by 2021
Original Phishing Scams - What do you notice about them?

Naomi Surugaba [a@.gov.my]

Inbox

Dear Beloved Friend,

I know this message will come to you as surprised but permit me of my desire to go into business relationship with you.

I am Miss Naomi Surugaba a daughter to late Al-badari Surugaba of Libya whom was murdered during the recent civil war in Libya in March 2011, before his death my late father was a strong supporter and a member of late Moammar Gadhafi Government in Tripoli. Meanwhile before the incident, my late Father came to Cotonou Benin republic with the sum of USD4, 200,000.00 (US$4.2M) which he deposited in a Bank here in Cotonou Benin Republic West Africa for safe keeping.

I am here seeking for an avenue to transfer the fund to you in only you’re reliable and trustworthy person to Investment the fund. I am here in Benin Republic because of the death of my parent’s and I want you to help me transfer the fund into your bank account for investment purpose.

Please I will offer you 20% of the total sum of USD4.2M for your assistance. Please I wish to transfer the fund urgently without delay into your account and also wish to relocate to your country due to the poor condition in Benin, as to enable me continue my education as I was a medical student before the sudden death of my parent’s. Reply to my alternative email:missnaomisurugaba2@hotmail.com, Your immediate response would be appreciated.

Remain blessed,
Miss Naomi Surugaba.
Your company is at **risk** if you…

- Have certain letters in your domain name
- Accept resumes on your website
- Highlight your Management or Leadership Team on your website
- Have a LinkedIn profile
- Think your life is deemed *interesting* enough to be on Facebook
It Only Takes One.
Introducing: Your Users

Laura
February 9 at 3:08pm

I just helped a member unlock his online banking and he decided to make his new password LAURA123 because why not?! TGIF 😅

Jess

Hahaha amazing! I always change it it whatever season it is with the year at the end but that sounds like a better tactic 🤖

Like · Reply · 3w

Jess replied · 2 Replies

Shannan
What bank do you work for?

Like · Reply · 3w

Laura Credit Union 😊
Would You Click?

Hello Chase Online™ Customer,

We are sorry, due to several failed attempts to access your account, we have temporarily deactivated your account for your protection. You are required to reactivate your bank account within the next 48 hours in order to continue using it.

Please logon to www.chase.com and enter your information correctly.

We apologize for any inconvenience this may have caused and look forward to taking further action with you to ensure your account remains secure.

Please do not reply to this automatically system generated email.

Sincerely,
-Your Chase Online™ Banking Team
This Is A Wicked Bad Site

YOU SHALL NOT PASS
WSYUD?

What Should Your User Do?
Do you think the link is safe?

We've randomly selected this link for training purposes. Review the details before deciding whether it's safe.

**Link Clicked**

**Message Subject**
Your Chase Account Has Been Compromised

**Message Sender**
Bob Adams

**Email Address**
abuse@ medic.com

[It's Safe] [It's Harmful]

Targeted Threat Protection
Your decision will be logged for tracking and audit purposes.
Sorry, this link is harmful

In future, please check links carefully before proceeding. You can close this page.

Safety Tips

Be suspicious of requests to transfer money, even if they look genuine. Always check with the company directly, using the contact details on their website rather than in the message.

Targeted Threat Protection

Your decision will be logged for tracking and audit purposes.
Real or fake?
Is this really Apple.com?

That “Apple.com” URL is really this…

xn--80ak6aa92e.com
Watch Out Mobile Browsers!
Phishing with Elongated URLs – What site are you really on?

http://m.facebook.com--------------------------securelogin.liraon.com/sign_in.htm
Would You Open This Attachment?
Ooops, your files have been encrypted!

What Happened to My Computer?
Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don’t pay in 7 days, you won’t be able to recover your files forever. We will have free events for users who are so poor that they couldn’t pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.
No One Way to Catch Malware
We all know the risks

Trust your users not to click?

Imagine being able to stop *EVERY* malicious file
Static File Analysis

Expedites scanning and scan time for users

~1-2 seconds attachment scan
Analyze inbound attachments with multiple AV engines + static file analysis + behavioral sandboxing + Safe file conversion
Enhanced Threat Remediation

• Leverage global threat intelligence
• Incident / Response Dashboard
• Constantly monitor and re-check status of all file attachment fingerprints globally
• If security score of a delivered file changes:
  – Quickly alert and update administrators
  – Automatically or manually remediate attachment based malware
  – Log incident actions
Who Says Attacks Need to Involve Malware?

- Business Email Compromise
- Whaling
- Wire transfer or W-2 Fraud
Who would send the money?

---

From: Peter Campbell [mailto:pcampbell@mircast.com]
Sent: Wednesday, July 29, 2015 10:46 AM
To: Peter Fondini
Subject: RE: Payment Request

Peter,

Find attached wiring instructions for a wire of $48,254.80. I need you to process this, code to Professional Service expenses and send me confirmation when completed.

This ought to have been sent yesterday.

Thanks,

Peter
From: Peter Campbell [mailto:pcampbell@mircast.com]
Sent: Wednesday, July 29, 2015 10:46 AM
To: Peter Fondini
Subject: RE: Payment Request

Peter,

Find attached wiring instructions for a wire of $48,254.00. I need you to process this, code to Professional Service expenses and send me confirmation when completed.

This ought to have been sent yesterday.

Thanks,

Peter
From: Peter Campbell [mailto:pcampbell@com]
Sent: Wednesday, July 29, 2015 5:09 PM
To: Peter Fondini
Subject: RE: Payment Request

Peter--what is the update of the wire

Thanks,

Peter
Impersonation
Protect

Whois Record (last updated on 2015-08-02)
Domain Name: MIRNECAST.COM
Registry Domain ID: 1949875411DOMAIN.COM-VRSN
Registrar WHOIS Server: whois.tucows.com
Registrar URL: http://tucowsdomains.com
Updated Date: 2015-07-29T13:06:40Z
Creation Date: 2015-07-29T13:06:40Z

From: Peter Campbell [mailto:pcampbell@irne.com]
Sent: Wednesday, July 29, 2015 5:09 PM
To: Peter Fondini
Subject: RE: Payment Request

Peter--what is the update of the wire

Thanks,

Peter
Supply Chain Impersonation
One of these things is not like the others!!!
“Similar” Domains Being Registered Every Day – Why?

- Serer - facebook.com - xn--faebok-ozb.com [facebook.com]
- Old English - apple.com - xn--le-m1aa24e.com [apple.com]
- Math Symbol - hotmail-.com - xn--hotmail-jka.com [hotmail.com]
- German - microsöftonline.com - xn--microsftonline-0pb.com [microsoftonline.com]
- Chinese - amazon.购 物 - amazon.xn--g2xx48c [amazon.com]
- Cyrillic - appleך.com - xn--appl-t64a.com [apple.com]
- Polish - aşure.com - xn--aure-bbb.com [azure.com]
- Fula/African - dropbox.com - -dropox-sxc.com [dropbox.com]
- Fula/African - ebay.com - xn--eay-osb.com [ebay.com]
- Polish - ebąy.com - xn--eby-jpa.com [ebay.com]
- Danish - facebøøk.com - xn--facebk-fyaa.com [facebook.com]
## Similarity matching capabilities

<table>
<thead>
<tr>
<th>Real Domain</th>
<th>Similarity Match</th>
</tr>
</thead>
<tbody>
<tr>
<td>mimecast.com</td>
<td>mimecast.co.za</td>
</tr>
<tr>
<td>apple.com</td>
<td>xn--80ak6aa92e.com</td>
</tr>
<tr>
<td>amazon.co.uk</td>
<td><a href="http://www.amazonn.co.uk">www.amazonn.co.uk</a></td>
</tr>
<tr>
<td>facebook.com</td>
<td><a href="http://m.facebook.com----------------------------------">http://m.facebook.com----------------------------------</a></td>
</tr>
<tr>
<td>paypal.com</td>
<td><a href="http://m.facebook.com----------------------------------">http://m.facebook.com----------------------------------</a></td>
</tr>
<tr>
<td>CustomDomain.com</td>
<td>CustomDomain.com</td>
</tr>
</tbody>
</table>

- Detect similarity both simple and complex
  - Character switching, Homoglyph/Homograph, long domain strings and more
Are Users part of the solution or part of the problem?

Internal Email Protect

- **Compromised Accounts**
  - Attacker uses stolen user credentials to spread attack internally and/or externally

- **Careless Users**
  - “Oops, I sent it to the wrong person...again.”

- **Malicious Insiders**
  - Purposely distributing malware or malicious URLs
Cyber Resilience for email