Cutting the Phishing line

James Spiteri
Solutions Architect, Security Specialist
Solutions Lead
Phishing

https://liscio.me/how-to-prevent-phishing/
The (traditional) Problem

From: Bank of America <crvdi@comcast.net>
Subject: Notification Irregular Activity
Date: September 23, 2014 3:44:42 PM PDT
To: Undisclosed recipients:
Reply-To: crvdi@comcast.net

Online Banking Alert
Dear member:

We detected unusual activity on your Bank of America debit card on 09/22/2014. For your protection, please verify this activity so you can continue making debit card transactions without interruption. Please sign in to your account at https://www.bankofamerica.com to review and verify your account activity. After verifying your debit card transactions we will take the necessary steps to protect your account from fraud. If you do not contact us, certain limitations may be placed on your debit card.

© 2014 Bank of America Corporation. All rights reserved.
Log in to your PayPal account

Not Secure | paypal--accounts.com

Email or mobile number

Password

Log In
The (nextgen) Problem

We want to make sure you're the owner of this account

We didn't recognise a device or location that was recently used to log in, so we'd like to confirm your identity.

To help protect your account we regularly look for early signs of potentially fraudulent activity.

Just to be safe, we want to make sure that this is your account. If this is not your transaction, we will help the process of recovery refund and protect your account. Pressing the button below

Recovery My Account
Why?

Let's Encrypt

Cloudflare
What can I do about this?

TELL ME HOW!
Enter Certificate Transparency Logging

https://www.digicert.com/certificate-transparency/how-it-works.htm
What does it attempt to solve?

- Rogue or Compromised CA
- Unauthorised certificate issuance in our organisation
- Auditing and Monitoring
TL;DR

There is a secure, publically available log for every TLS certificate signed by a trusted authority!
But, is it enforced?

Yes!

Apple Announces Certificate Transparency Requirement

Chrome Browser Now Enforces Certificate Transparency

By Ionut Arghire on May 02, 2018

Effective May 1, Google’s Chrome browser will display a warning when encountering certificates that are not compliant with the Chromium Certificate Transparency (CT) Policy.
Ok, so how can I use CT logs to my advantage?

Search.

Demo Setup
Other Services

Certificate Transparency Monitoring Beta
Receive an email when a Certificate Authority issues a certificate for your domain.

Notification email
Add

Your free trial ends on 2020-02-12. To continue receiving alerts about uptime and security problems, choose a plan before this date.

6 Monitored Endpoints
0 Endpoints with Expiring Certs
4 Discovered Certificates
4 Unknown Certificates
Settings

Orders Cert Spotter Account

2 new certificates for [mask] or its subdomain were issued by Let's Encrypt Authority X3.
2 d
Wrapping up - CT Logs allow us to:

- Detect **new** certificates for our domains
- Search for certificates which can potentially be used for **phishing campaigns**
- **Correlate** against other log sources
- Create **reports** of certificate generation activity
- Track **expiry**
- **Enumerate** subdomains
- And more..

Security Bot APP 10:52 AM
SwiftCrypto Alert

New Certificate Detected
1 New certificates have been created according to certificate transparency logs in the last minute.

DNS Name: portal.swiftcrypto.com, Certificate Issuer: Let's Encrypt,

CT Log Entry: https://ct.googleapis.com/logs/argon2019/,

@James Spiteri has acknowledged this incident. Apr 16th
Thank You!

Credits:
https://elastic.co
https://certstream.calidog.io
https://github.com/SSLMate/certspotter
https://blog.cloudflare.com/introducing-certificate-transparency-monitoring/
https://ct.cloudflare.com
https://crt.sh
https://censys.io
https://www.digicert.com/certificate-transparency/how-it-works.htm
https://letsencrypt.org