Email is the Top Attack Vector for Social Engineering Attacks

96% of Social Attacks Use Email

Even as attackers expand to new vectors, Email must be a top priority

88% YoY Rise in Business Email Compromise

22% of employees will click on a phishing link

Source: Verizon Data Breach Report & FBI IC3 Annual Report
Cybercriminals can Easily Take-on a Persona to Exploit Victims

Inbox

Next: No events for the next two days.

Filter

Agenda

Ravi Khatod
Urgent
5/10/2017
Hi Raymond. Are you available to move quickly today? I ...

Urgent

Familiar Request

Authoritative Figure

Existing Relationship

Raymond,  
Are you available to move quickly today? I need you to be ready to process a wire transfer and I want the money to hit the beneficiary account before the bank cut-off time today. As you know, I’m at a conference today, so I can give you the details when I get back to the office. Get back to me ASAP.

Thanks,
Ravi
While Content Analysis can Discover Intent & Attacker Insight…. 

Unsolicited Scam

From: Mohammad Abacha
To: Raymond Lim (CFO)
Subject: Offer Only for Today

Dear Sir/Madam,
I am Mohammed, the son of the late Nigerian Head of State. Please, I need your assistance in recovering huge sums of money deposited by my father…..

Business Email Compromise

From: Ravi Khatod (CEO)
To: Raymond Lim (CFO)
Subject: Urgent Request

Hi Raymond,
Are you available today to move quickly today. I need you to process a wire transfer today and I want the money to hit the beneficiary account before the bank cut-off…..

… To Justify Further Actions
Modeling Sender Identity & Behavior Can Lead to Faster Prevention

Map and Authenticate Identities

Learn and Model Behavioral Relationships

Score Message vs. Expected Behavior
Making Phishing Prevention More Efficient

Exact Domain Spoof
From: Lisa Su <Lisa.Su@amd.com>
To: Brian Krzanich <BrianK@intel.com>
Subject: Partnership Agreement

Attackers Leverage: Public Cloud Infrastructure

Display Name Deception
From: Chase Support <chase@gmail.com>
To: Tom Frost <ffrost@amazon.com>
Subject: Account Disabled

Attackers Leverage: Free Webmail Providers

Compromised Account
From: Raymond Lim <rlim@contoso.com>
To: Cong Ho <cho@contoso.com>
Subject: PO 382313

Attackers Leverage: Phishing, Weak Passwords

Look-Alike Domain
From: LinkedIn <noreply@liinkediin.com>
To: Jan Bird <jan.bird@gs.com>
Subject: Diana has endorsed you!

Attackers Leverage: Cheap Domain Registrars

Source: Agari Business Email Compromise Attack Trends Report
Ultimately, Using In-Depth Email Analysis Expands Protection

**Identity & Behavioral Relationships**
- Protect the most exploited attack vector to prevent phishing attacks

**Email Text & Artifacts**
- Enables response & cooperation with authorities to prosecute cybercrime

**Text**
- Expands protection to non-email based attack vectors
Next Steps

Connect with Agari at Black Hat:

Stop by Booth #600

Attend an Agari Live Session at Black Hat Europe

Title: Understanding the Criminal Mind
How Western European BEC Syndicates Leverage Business Intelligence

Date/Time: Wednesday, Dec. 5, 2:55pm-3:30pm

Learn More About Defending Against Social Engineering:

Agari.com/social-engineering
Thank You

AJ Shipley
ashipley@agari.com
www.agari.com
@agariinc