Agenda

- Introduction
  - Speakers: Peter Cholnoky, Arnie Bjorkland; E-HAWK
  - Tara Natanson, Gene Gusman, Sweeney Williams, Andrew Bonar
- What is vetting? Why do you need to do it?
- Stopping the “real” bad guys
- Stopping the “accidental” bad guys
- What to do when you miss a bad actor
- Questions
E-HAWK

- Peter Cholnoky, CEO / Arnie Bjorkland, VP sales

- Born out of MAAWG. Founders from SURBL and cyber security
- Goal of creating a service to keep out bad actors

- Vetting Service now live and in production with large ESPs
  - Identifies risk areas of sign-ups and users by automating hundreds of tests
  - Community data shared to help tune scoring and stop account hopping

- How it Works
  - API call with user data -> JSON Risk Score
  - Processed over 800k vets, 150k community
What is vetting? Why do it?

The Goal of Vetting
- Create an effective and efficient on-boarding process that limits risk and accelerates sales
- Keep out bad actors – they impact reputation, cost money and time to stop and fix
- Focus sales teams on real opportunities vs. scams

The Challenges
- ESPs are in the business of selling email services, not vetting
- Vetting can be complicated with a lot of tests, both on individual data and linked data
- The bad actors change tactics and it’s a cat and mouse game trying to keep up
- No vetting process or system is perfect. But, a good vetting process will keep out very bad actors who significantly impact your business and reputation
Some Stats from E-HAWK Vetting

Our Experience and Findings (as of Oct 2013)

(800k+ vets, 10M+ tests processed, 150k+ in community data)

- 83% of vets from Lowest to Some Risk
- 17% are Medium to Very High Risk
- 3% are Very High Risk
- Risk needs to be factored from multiple data points
  - 30% have some risk with IPs
  - 25% have some risk with email or domain
  - 20% have some risk with geo or location
  - 5% hitting community
  - 2,400 activity/frequency entities in 11 days

- An Interesting Find
  - 110 emails in a frequency incident. At 10K emails per account = 1.1M spam messages
2 Types of Bad Actors

Malicious / Criminal
- Companies
- Gangs
- Consumers

Primary purpose is to leverage your platform as a delivery mechanism for their criminal activity

Ignorant / Misguided
- Buy lists
- Send improper content
- Typically companies or consumers
- “Don’t know what they are doing”
- Ask for forgiveness, not for permission
Stopping the “real” bad actors

- Overview – The basics
- Member examples
  - The self-serve model
  - Others
Vetting Process Example

- **Individual Testing of Variables for Risks**
  Example: test IP for proxy, SPAM lists, known fraud, etc.

- **Frequency Testing for Patterns**
  Example: has this “data” been active on other signups or use?

- **Combined Testing for Risks**
  Example: does the phone and IP location look OK together?

- **Community Testing for Risks**
  Example: has this data be reported by others in the network?

**Risk Level**

Email Sender & Provider Coalition
Vet Scoring Process

- Start each test at Zero
- When your find good things like a clean IP, add a few points
- When you find bad things like a history of spam, subtract a bunch of points
- Risk Score should be based on 3+ data points and many tests
- Risk Score is a point in time and changes quickly – re-vet often

- Define risk policies that align with scoring thresholds for your business.
Verify vs. Vetting

**Verify**
Does this email exist on the server?

gec01@gecmarrakech.com

**Vetting**
Is this email or domain associated with risk? Is there a spam, fraud, or phishing history?

The email exists and is valid.

The email and domain have a history of trying to create multiple accounts using gec01, gec02, gec10 and has been identified with fraud. Consider high risk.

Simple verification is not enough to combat bad actors into today’s environment.
# Vetting Individual Data Points

## Vetting IP

On sign-up forms, the IP is something end users cannot lie about and should be vetted thoroughly

- Check for any history or activity on blacklists
- Check IP location for high risk
- Check IP for proxy, TOR, black VPNs or other risky elements

Vetting strategies: use public and private data to check for risk

- IP DNSBL Services
  - SPAMHAUS
  - SPAMCOP
  - URIBL BLACKLIST
  - SORBS
  - SWINOG URIBL
  - MAILSPIKE
- Geo Services
- IPADDRESSAPI
- Private Services

## Vetting email

Email address provides many areas to vet

- Check if from free services (gmail, yahoo, qq, etc.)
- Check on history of email. Is it associated with fraud, scams, etc. Check email blacklists
- Take domain from email address and run domain testing
- Cross check for email history of previous accounts, sign-ups, or fraud
- Verification of email address to start account does not help with bad actors

Vetting strategies:

- Maintain a list of free email services with risk levels
- Search public and private email blacklists for both email and email domain activity
- Incorporate a lookup of past account activity for the email and email domain to flag repeat offenders

## Vetting Phone

Phone can provide insight to location and validity of user

- Verify the number is real and not made up
- Check for history of crime or fraud
- Check if number is forwarded
- Check if number is un-allocated

Vetting strategies:

- Use public or private phone verification databases to check for validity and location
- Incorporate a lookup of past account activity for the phone number to flag repeat offenders
# Vetting Individual Data Points

## Vetting Location

Location (address, city, state, postal code and country)
- For US, check if state and postal code match
- Check location for risk
- Check for history of crime or fraud

**Vetting strategies:**
- Use public or private address verification databases to check for validity and proper correlation between items
- Maintain a location list with risk levels

## Vetting Domain

Domain can provide insight into the user and legitimacy
- Verify domain exists and has a clean record
- Check for domain age - newly created domains are suspect
- Check domain modification for recent changes
- Check domain country

**Vetting strategies:**
- Use public or private domain lookups (whois) to find domain age, modified dates, and owners
- Use lookup services for domain blacklists
- Maintain a country list with risk levels to associate with domain countries
Stopping the “accidental” bad actors

- Overview – The basics
- Member examples
  - On-boarding at the enterprise level
  - More on self-serve models
  - Community aspects
  - Other
Vetting Activity – Frequency Testing for Patterns

Activity patterns can identify phishers, bots, and high risk users

- Check for patterns in emails jim1@domain.com, jim2@domain.com, jim3@domain.com
- Check for patterns in IP (1.1.1.1, 1.1.1.2, 1.1.1.3)
- Test for patterns across domains, phones, and locations

Vetting strategies:

- Track short-term activity for repetitive patterns of key data points
- When identified, link all history to remove threat. Example: when seeing repetitive emails, all current and past similar emails need to be tagged.

Effective for combatting Waterfalling and Snowshoe Spamming Tactics.
Vetting Geo-location

Geo data should be analyzed for consistency

- Create group checks, such as “Does the IP location make sense with the location data?”

Vetting strategies:

- Track as much geo data as possible
- Run region analysis and testing against groups of data that should be similar.
  Rank matches positive and miss-matches negative
- Use region and country risk factors in analysis

Email: jim@yahoo.com.br
IP: from China
Phone: Ohio
Domain: xxx.br
Address: Florida, US
Community Data

Bad Actors jump between ESPs, already have “sleeping cells” in many accounts, and are very actively

- Vet and review all new sign-ups
- Vet all account updates to prevent account hijacking and Adobers re-do
- Vet all account owners before campaigns launch to see if they are high risk

Vetting strategies:

- Be proactive and share data with partners, competitors, and trusted third parties. We all have one enemy = Bad Actors
- Ensure your sharing data is ranked by category, type
- Automate the sharing process – real-time data is more effective
On-boarding models

- Self-service / small list senders
  - Automated vetting based only on registration info for the account and begin mailing (no DNS/whois/BBB look-ups)
  - Heavily weighted towards the content of mailing list and secondarily the content of individual campaigns

- Larger senders / B2B
  - Manual vetting done by human research
  - Remediation performed following initial sends
More examples

- Other tools
- What to do when you miss a bad actor
  - Why you might miss a bad actor
  - What you can do on a going forward basis to catch any bad actors you might miss initially
Questions