Constella

DATASHEET

# Scam GPT

## Build Next-Gen Defenses to Protect Against New Hyper-targeted AI Scams

Warren Buffett predicts that AI-driven scams are poised to become the next major “growth industry,” presenting both immense opportunities and significant risks.

Criminals are now leveraging sophisticated tools such as FraudGPT and WormGPT on the dark web to orchestrate advanced scams using generative AI techniques, posing challenges that current security measures struggle to match. This escalating threat underscores an urgent demand for innovative human defenses capable of effectively countering and mitigating these evolving risks.

### Protect Against the Scam AI Wave Through Enhanced Human Defenses

The only true protection to these scams is to enhance human defenses through education and training on how compromised user information can be used by criminals to build seamless scam narratives to exploit them.

- Test your Employees:
  ScamGPT can send a series of emails or generate voice scam messages designed to test and train an organization’s employees. This method helps safely educate staff and raise awareness about scam tactics, thereby enhancing their ability to recognize and protect against real scams.
- Surface of Attack Awareness:
  Identity theft, antivirus, pen testing and cyber security services can offer a rich view of the surface of attack and risk profile of each user and include scam examples of each user vulnerability found.

### Simulating AI Scams with Real Compromised Identities

Constella’s ScamGPT is powered by the world’s largest data lake comprising 1 trillion+ identity assets, paired with the company’s proprietary ID Fusion AI profiling engine, which automatically generates the surface of attack from across surface, social, deep and dark web exposures.

- Surface of Attack:
  Constella's ID Fusion creates the surface of attack composed of all the compromised identities belonging to one person.
- Hyper-targeted AI Scams:
  ScamGPT can generate millions of different scams processing the surface of attack using trained generative AI algorithms.
- Continous Protection:
  The solution can produce ongoing scams that include new exposed information from a user.

**Outputs:**

- **Surface of Attack:** List of all the exposed information from a user collected from the internet and the dark web.
- **Risk Profile:** List of the main risks that a user faces depending on his specific surface of attack.
- **Scams:** ScamGPT can send continuous scams to millions of users to educate, train and protect them.

# Scam GPT

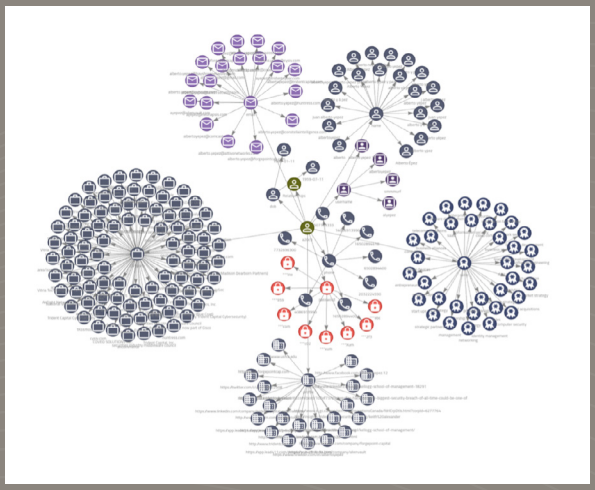
DATASHEET

## ScamGPT: Real-life Example

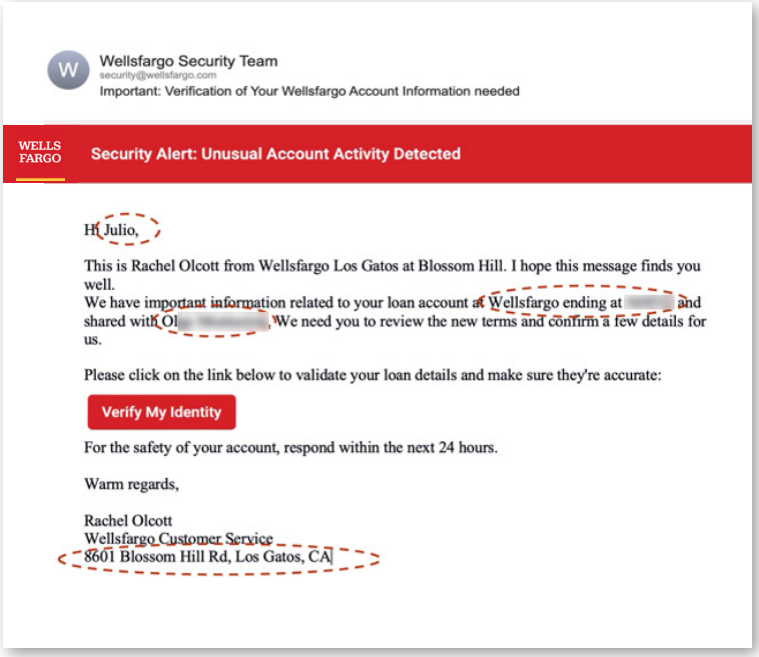
Julio Casal
Founder of Constella

ScamsGPT used 1 email for Julio to detect 152 attributes and produce more than 200 hyper-targeted scams:

- 13 emails
- 12 credentials
- 13 phones
- 31 skills
- 12 companies
- 5 addresses
- 54 relationships
- Bank information
- Car information



## Targeted Scams Generated with GenAI



Wellsfargo Security Team
security@wellsfargo.com
Important: Verification of Your Wellsfargo Account Information needed

WELLS FARGO — Security Alert: Unusual Account Activity Detected

Hi Julio,

This is Rachel Olcott from Wellsfargo Los Gatos at Blossom Hill. I hope this message finds you well.
We have important information related to your loan account at Wellsfargo ending at [redacted] and shared with Ol[redacted]. We need you to review the new terms and confirm a few details for us.

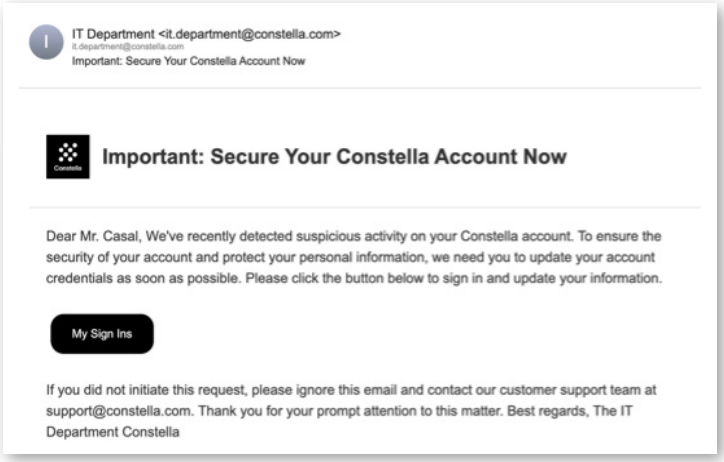
Please click on the link below to validate your loan details and make sure they're accurate:

Verify My Identity

For the safety of your account, respond within the next 24 hours.

Warm regards,

Rachel Olcott
Wellsfargo Customer Service
8601 Blossom Hill Rd, Los Gatos, CA



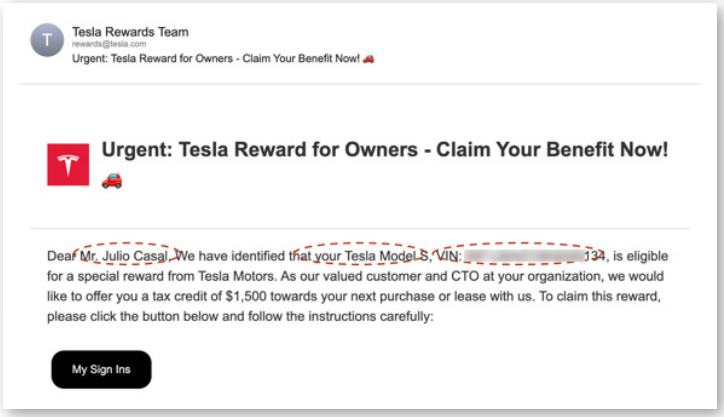
IT Department <it.department@constella.com>
it.department@constella.com
Important: Secure Your Constella Account Now

**Important: Secure Your Constella Account Now**

Dear Mr. Casal, We've recently detected suspicious activity on your Constella account. To ensure the security of your account and protect your personal information, we need you to update your account credentials as soon as possible. Please click the button below to sign in and update your information.

My Sign Ins

If you did not initiate this request, please ignore this email and contact our customer support team at support@constella.com. Thank you for your prompt attention to this matter. Best regards, The IT Department Constella



Tesla Rewards Team
rewards@tesla.com
Urgent: Tesla Reward for Owners - Claim Your Benefit Now! 🚗

**Urgent: Tesla Reward for Owners - Claim Your Benefit Now!** 🚗

Dear Mr. Julio Casal, We have identified that your Tesla Model S, VIN: [redacted]134, is eligible for a special reward from Tesla Motors. As our valued customer and CTO at your organization, we would like to offer you a tax credit of $1,500 towards your next purchase or lease with us. To claim this reward, please click the button below and follow the instructions carefully:

My Sign Ins

Protect Against Emerging Hyper-targeted AI Scams with Next-Gen Defenses

Learn more about Constella's ScamGPT Solution: Constella.ai

Constella

About Constella

Constella.ai is the global leader in AI-driven identity risk and deep and dark web intelligence for such applications as identity theft, insider risk, Know Your Employee (KYE), and deep OSINT investigations. With the world's largest breach database, containing over one trillion data attributes in 125+ countries and over 53 languages, Constella empowers leading organizations across the globe to monitor and secure critical data through unparalleled visibility and actionable insights. Ready for a secure future? Reach out to Constella today and stay one step ahead of digital threats.