

# Phishing, the Use of Cryptocurrency, and Staying Safe

Presented by Kevin A. McGrail



GBA

# Hello, everyone!



**Kevin A. McGrail**

Principal Evangelist at Dito

[in linkedin.com/in/kmcgrail](https://www.linkedin.com/in/kmcgrail)

Google Workspace TC, GDE, and Ambassador

Member, U.S. Marine Corps Cyber Auxiliary



# Think Evil

Start with Why:

- Threat Modelling is important.
- **MITRE** ATT&CK to understand your adversaries and their TTP (Tactics, Techniques & Procedures)
- Palo Alto Networks Unit 42 Playbooks

Read more Spy Novels



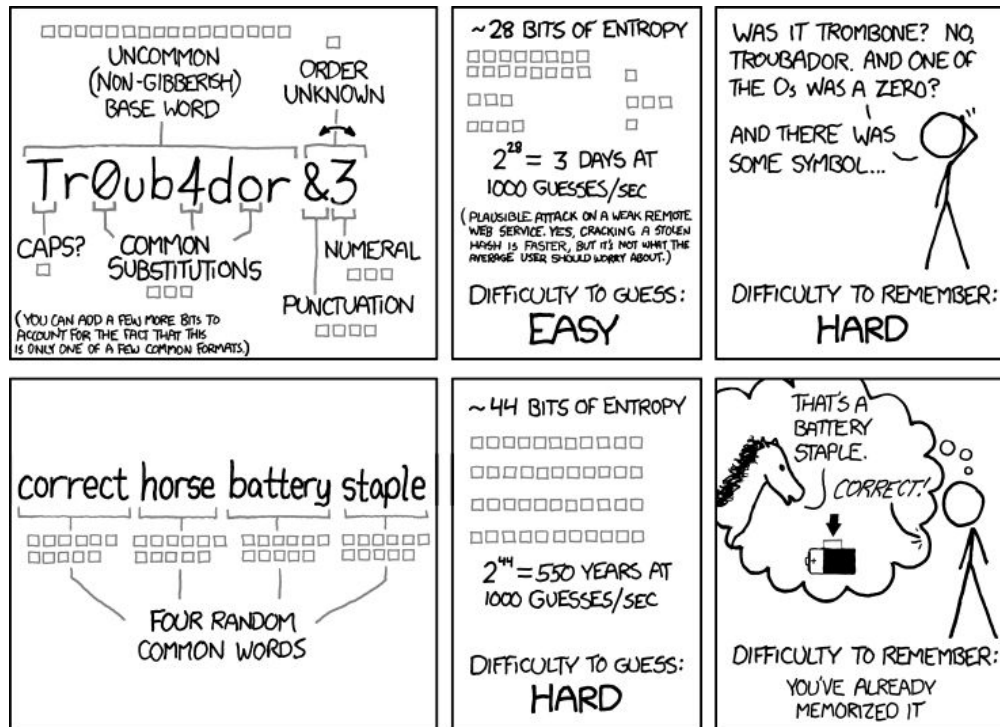
Google Cloud

# Use Passphrases

Get rid of password complexity and instead use passphrases

**National Institute of Standards and Technology (NIST)** Digital Identity Guidelines, [SP 800-63B Section 5.1.1.2](#) paragraph 9, “recommends against the use of composition rules (e.g., requiring lower-case, upper-case, digits, and/or special characters) for memorized secrets. **These rules provide less benefit than might be expected...**”

Don't require periodic password changes: “**Verifiers SHOULD NOT require memorized secrets to be changed arbitrarily** (e.g., periodically). However, verifiers SHALL force a change if there is evidence of compromise of the authenticator.”, SP 800-63B Section 5.1.1.2 paragraph 9



THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

# Cryptocurrency Benefits

The benefits of Cryptocurrency are also part of the problem:

- Ease of use
- Lack of Fiat controls
- Decentralized authority
- Anonymity(?)



# Psychology of Scams

## Nigerian Prince Scam

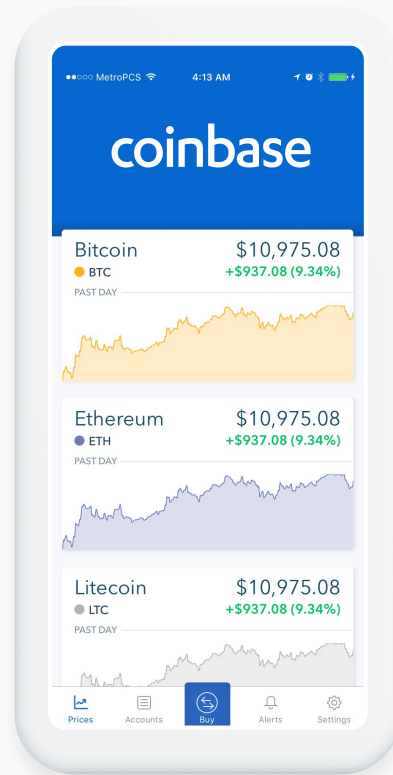
Try to separate logic from emotion, e.g.  
deadlines with severe penalties

Con Artists try to gain your Confidence



# Safe Use of Cryptocurrency

- Use good wallet management such as Coinbase
- Multi-factor Authentication
- Consider Crypto->Fiat conversions for purchases





# Cloud Resources are Targets

Fortune 1000 found crypto miners in their environment

Radarware: [Have Crypto-Miners Infiltrated Your Public Cloud?](#)

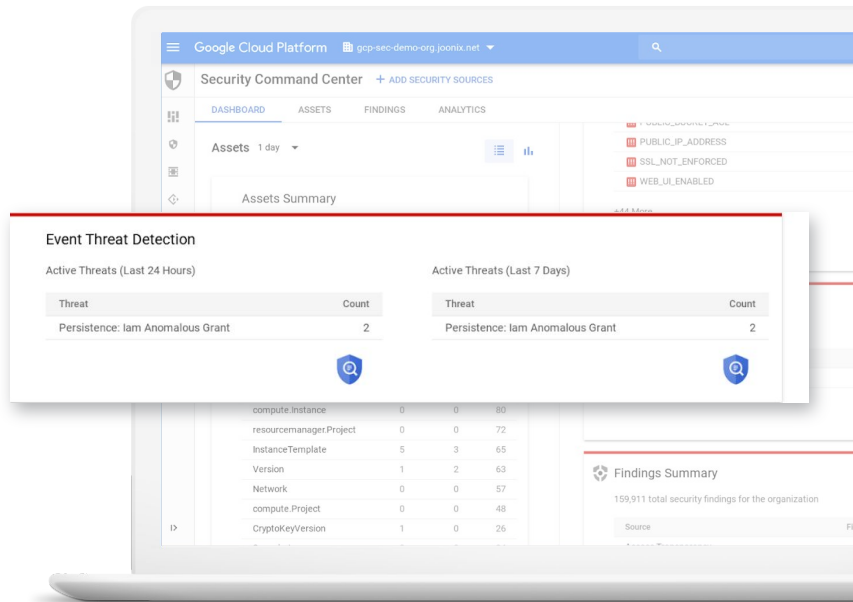


# How to Detect / Prevent Crypto Mining Malware

CSO online: [How to detect and prevent crypto mining malware](#)

Google Cloud Security Command Center

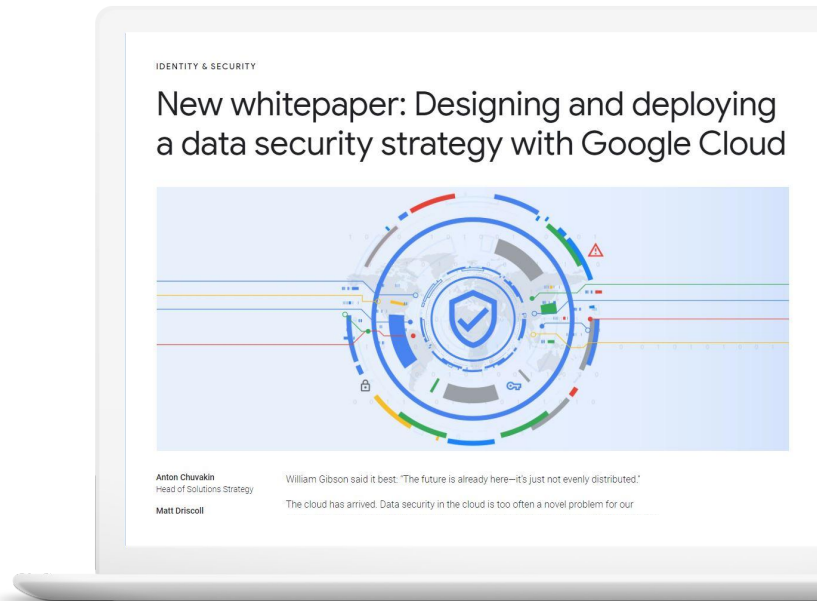
Google: [Detect and respond to high-risk threats in your logs with Google Cloud](#)



# Cloud Demands a New Strategy

New Cloud Strategy Whitepaper:  
[Designing your data security program  
in a cloud-native way on Google Cloud](#)

Treat your public cloud as a target



# Final Thought - Ransoms and Fall Out

- Committee on Foreign Investment in the United States (CFIUS)
- Anti-Terrorism Act (ATA)
- Primary and Secondary Liability
- The Lindbergh kidnapping

# Thank You

<https://www.linkedin.com/in/kmcgrail>

## Image Credits:

KAM photo taken by Ted King, used with permission

Blockchain Image: <https://pixabay.com/users/thedigitalartist-202249/>

Xkcd comic: <https://xkcd.com/936/>

Other stock images provided by Unsplash