

# KAM's Top 30 31 Modern Security Tips

Originally presented at Google Washington DC HQ Tech Talk, August 7th, 2018

Many of these tips are oldies but goodies to cyber security experts but I've tried to include a few unique tips with my personal explanation on each. Some of the tips are even a bit controversial but I've tried to give the important reason for "why". And while there is a tilt to help Google G Suite Admins, I'm happy to answer questions regarding how to secure any system using these tips.

As a bonus for those of you who attended my original presentation, I've included an extra tip! I hope you enjoy and feedback is welcome.

Thanks,

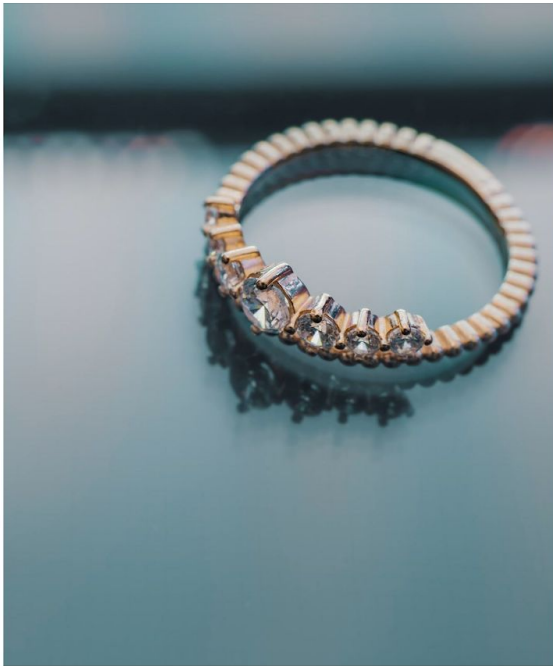
Kevin A. McGrail aka KAM

G Suite Expert (<https://developers.google.com/experts/people/kevin-a-mcgrail>)

G Suite Top Contributor (<https://topcontributor.withgoogle.com/profile/kevin-a-mcgrail-a5fc1d>)

Copyright © 2018, The McGrail Foundation, All Rights Reserved.

Licensed under CC BY-NC 4.0: <https://creativecommons.org/licenses/by-nc/4.0/>



#1



## Passphrases not passwords

Google Cloud

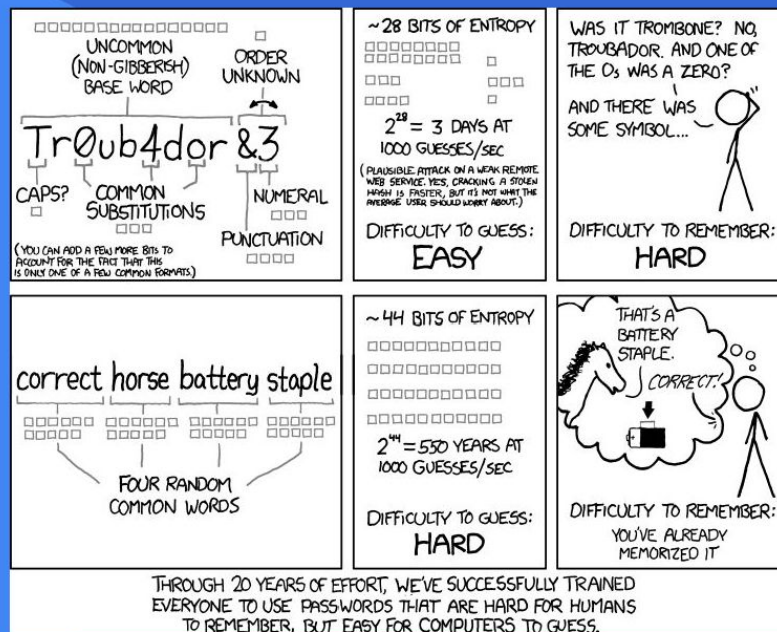
**Tip #1:** Passwords written down are inherently insecure so I recommend using passphrases that are easy to remember but infinitely too complex to brute force.

For example, a password of “MyWeddingAnniversaryIsJan12018” is not only very easy to remember but it can also help you remember your Wedding Anniversary.

# #2

## Password Length is Better Than Password Complexity!!

Google



**Tip #2:** Unless you are a hacker fluent in elite-speak, you probably find it difficult to remember passwords with those crazy complexity rules and letter substitution. Uppercase, special characters, numbers, etc. It gets more complex in places like the United Kingdom where they can't use common symbols £ in passwords.

The answer? Use long passwords which builds on my first Tip and ignore complexity.

XKCD comics does a wonderful job of explaining the scientific reasoning and shows how password complexity is completely dwarfed by password length for security. Plus the website <https://xkpasswd.net/> has a great tool for passphrase generation.

Just in case you don't trust a technogeek comic strip, the 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..."

# #3

“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

*Don't Require Password Changes*



**NIST**  
National Institute of  
Standards and Technology  
U.S. Department of Commerce



**Tip #3:** June of 2017 brought a big change to password management. ***NIST no longer recommends and explicitly acknowledges that routine password changes make your systems LESS secure.***

I can't say it any better than NIST did in their Frequently Asked Questions:

“Users tend to choose weaker memorized secrets when they know that they will have to change them in the near future. When those changes do occur, they often select a secret that is similar to their old memorized secret by applying a set of common transformations such as increasing a number in the password. This practice provides a false sense of security if any of the previous secrets has been compromised since attackers can apply these same common transformations.”

<https://pages.nist.gov/800-63-FAQ/>

So hopefully you're now convinced that long passphrases without the need to routinely reset them provides better security.

## Use Unique Passwords!!

#4

havebeenpwned.com

Base Password + Cipher (pig latin/Caesar/middle letters of site)



';--have i been pwned?

Google Cloud

**Tip #4:** Unique passwords are important. I recommend using a simple cipher for a website plus a base passphrase. For the cipher, use something simple such as a Caesar cipher or just writing the first & last letter in a website name in pig latin. It doesn't take much to avoid the damage from one compromised site.

Want to explain to your users why unique passwords are important? Sign up for havebeenpwned.com. They use information from data breaches to let you know if you have accounts that are affected on your domain. And they can give you ongoing alerts.

For example:

## An email on a domain you're monitoring has been pwned

You signed up for notifications when emails on **redacted** were pwned in a data breach and unfortunately, it's happened. Here's what's known about the breach:

<b>Breach:</b>	Exactis
<b>Date of breach:</b>	1 Jun 2018
<b>Accounts</b>	131,577,763

**found:**

**Your accounts:** 10

**Compromised data:** Credit status information, Dates of birth, Education levels, Email addresses, Ethnicities, Family structure, Financial investments, Genders, Home ownership statuses, Income levels, IP addresses, Marital statuses, Names, Net worths, Occupations, Personal interests, Phone numbers, Physical addresses, Religions, Spoken languages

**Description:** In June 2018, [the marketing firm Exactis inadvertently publicly leaked 340 million records of personal data](#). Security researcher [Vinny Troia of Night Lion Security](#) discovered the leak contained multiple terabytes of personal information spread across hundreds of separate fields including addresses, phone numbers, family structures and extensive profiling data. The data was collected as part of Exactis' service as a "compiler and aggregator of premium business & consumer data" which they then sell for profiling and marketing purposes. A small subset of the exposed fields were provided to Have I Been Pwned and contained 132 million unique email addresses.

You can see which of the accounts you're monitoring were compromised by running another domain search.



#5

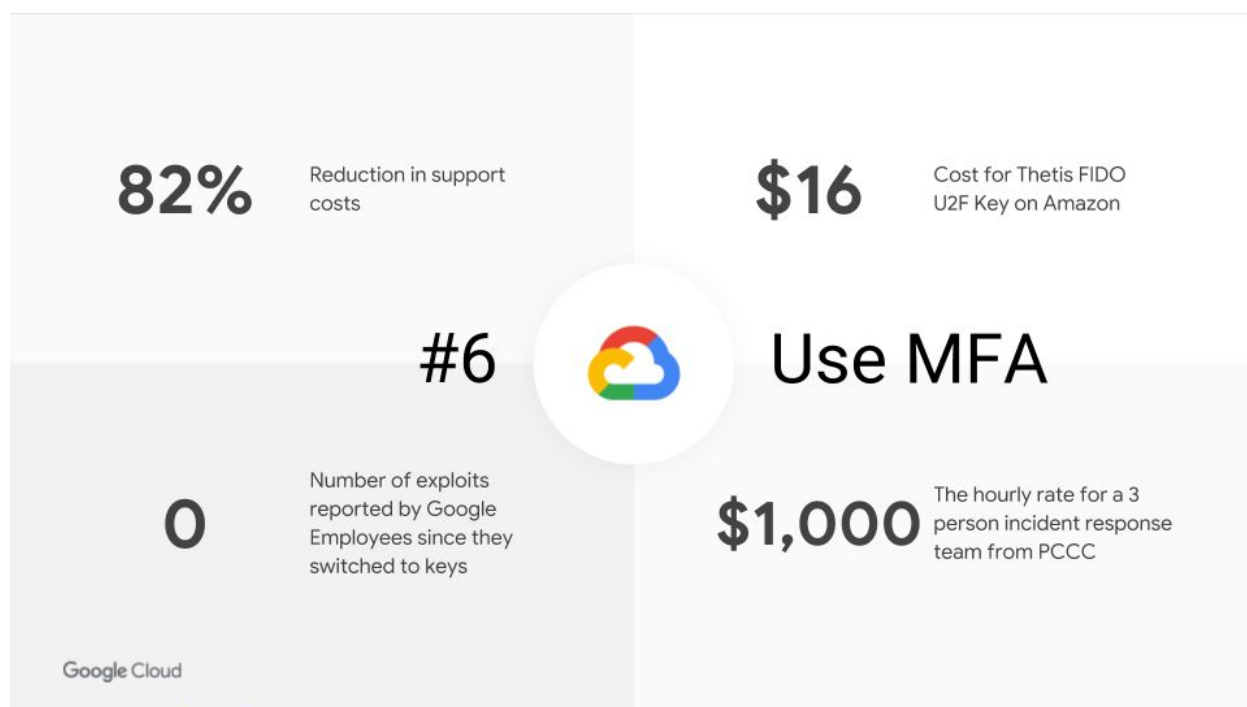
**You can't  
uncompromise  
biometrics.**

**Tip #5:** Don't use biometric protections. If they are compromised, you can't change them and they are pretty trivial to compromise.

First, as reported by The Guardian, <https://www.theguardian.com/technology/2014/dec/30/hacker-fakes-german-ministers-fingerprints-using-photos-of-her-hands>, Hacker Jan Krissler used high resolution photos, including one from a government press office, to successfully recreate the fingerprints of Germany's defence minister. Yes, I know that's a picture of Chancellor Merkel but it was hard to find a picture of Ursula von der Leyen with rights to use.

Second, fingerprints left on smart phones themselves have been used to trick fingerprint scanners using methods as simple as a black and white laser print and some Elmer's Glue.

Finally, my son's face will unlock my Apple Face ID which according to Wired must not be all that rare: <https://www.wired.com/story/10-year-old-face-id-unlocks-mothers-iphone-x/>



**Tip #6:** In early 2017, Google required security keys for all 85,000 of their employees. Since then, the number of exploited accounts is 0.

Use Multifactor Authentication! It is inexpensive, it works and the cost-savings are very clear.

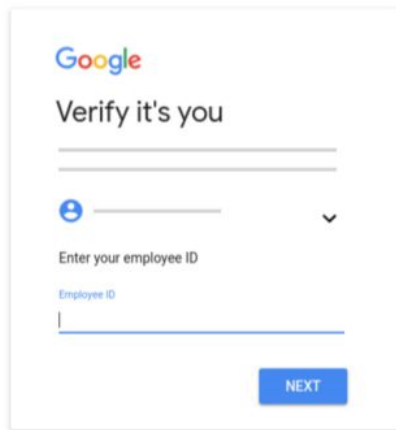
Yubico has keys that are FIPS 140-2 validated and made in the USA. Google also has their own Titan Keys coming out.

Just search FIDO U2F on Amazon for tons of options. Roll them out starting with your executives and administrators today.



## Add Google's Employee ID Login Challenge

#7



A screenshot of the Google login challenge interface. At the top is the Google logo. Below it, the text 'Verify it's you' is displayed. There are two horizontal lines for input. Below these is a blue circle icon with a white person silhouette, followed by a dropdown arrow. The text 'Enter your employee ID' is shown. Below that is a label 'Employee ID' and a text input field. At the bottom right is a blue button labeled 'NEXT'.



Google Cloud

**Tip #7:** Google just rolled out Employee IDs as a login challenge. Looking for a simple multifactor authentication with a light lift? Find out more here:

<https://support.google.com/a/answer/6002699?hl=en>

## Use Google Authenticator

“Two-factor authentication (2FA) that uses SMS or phone calls is only slightly better than no 2FA at all.”



Google Authenticator

Dan Goodin

*Ars Technica*

#8



**Tip #8:** If you can't use security keys, use the Google Authenticator app. It's free and available for Android, IOS and Blackberry.

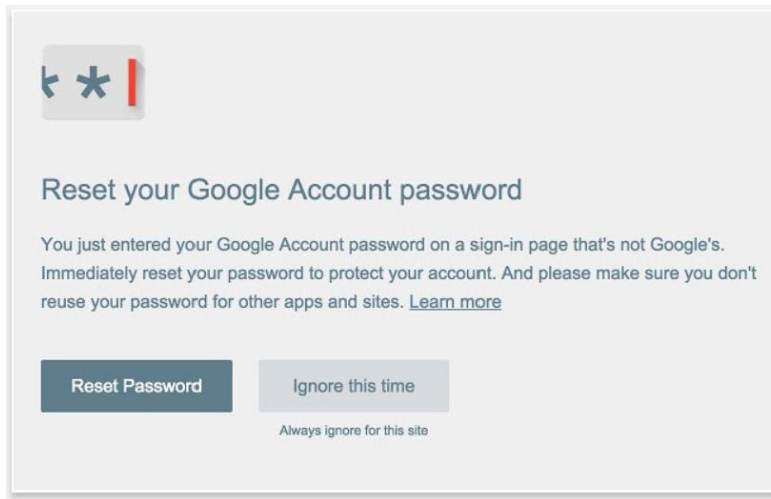
However, please do not use SMS or Text Messaging for your multifactor authentication. Signaling System No 7 (SS7) or Common Channel SS7 is the technology that connects one mobile phone carrier to another. It allows interoperability of texts between carriers and it is highly insecure.

Reddit's recent compromise is a textbook example of the issue as reported by Ars Technica, <https://arstechnica.com/information-technology/2018/08/password-breach-teaches-reddit-that-yes-phone-based-2fa-is-that-bad/>

#9

## Password Alert

Also alerts you about pages that are impersonating a Google sign-on page!



**Tip #9:** This Chrome Extension alerts users when they use their Google Account password on a non-Google site and helps users avoid being phished if the site they are on is impersonating a Google login page. It's a very simple task to install!

<https://chrome.google.com/webstore/detail/password-alert/noondiphcddnnabmjcihcjfbhfklnnep?hl=en>



## Users Can Be a Strong Link

Users **CANNOT** identify all scams. Encourage Help Desk Use!

Look for “Tip of the Iceberg” issues & pay attention to users who file good trouble tickets.

Encourage users to get those 10 seconds they need to separate the Emotion from the Logic.

Google Cloud

**Tip #10:** Users are routinely called the weakest link in security. However, I believe users can be a very strong security link in the chain. As an administrator, I take the stance that users can do no wrong. It is my job to select, develop & implement technology that protects users 100%.

This means I don't look to “train” users to identify scams. That's a false sense of security because as a security expert, I routinely see scams that take considerable time for me to identify. If it takes me even minutes as an expert, how can I expect users to do so effectively?

To me, the most important part is to 100% encourage help desk use. A user should do NOTHING if they feel something is amiss. Get the professionals involved early and look for those users who are often early indicators of larger issues when they report a problem.

Finally, most scams try and impart a sense of urgency on their target victims. Do this now **or else!** They do this to separate your logical mind from your emotional mind. All it takes is a 10 second pause for a mark to realize they are being conned. The number one phrase I hear doing incident response is “I knew immediately I shouldn't have done that.” Encouraging help desk tickets is one simple way that allows for this reflection.



# #11, #12 & 13



## A - Setup DKIM & SPF

## B - Setup DMARC

## C - Look at Dmarcian and Virtru

Google Cloud

**Tips #11, #12 & #13:** First, a conflict of interest disclosure. I am an adviser at Virtru. However, in 25 years, they are one of two board invitations I have accepted. Virtru's email encryption uses nation-state grade security that was originally designed for interagency communications post 9-11. It gives users one click Simplicity to encrypt emails with unparalleled Control where even after you've sent the email, you can revoke access quickly and easily.

With that out the way, your first step is to setup DKIM and SPF. These technologies help prevent your domain names being impersonated by bad actors. Google G Suite makes this incredibly simple. If you don't know what DKIM or SPF are or how to set them up with G Suite, see <https://support.google.com/a/answer/174124?hl=en> & <https://support.google.com/a/answer/33786?hl=en>.

MXToolBox also has great tools to help create SPF records: <https://mxtoolbox.com/spf.aspx>

Next, after you implement DKIM & SPF, setup a DMARC record. The website <https://dmarcian.com/dmarc-inspector/> can help make sure it's valid and Dmarcian also offers a reporting platform for ongoing DMARC monitoring.

Finally, [virtru.com](https://virtru.com) provides simple and secure end to end encryption for email. You can get it in the G Suite Marketplace at

[https://gsuite.google.com/marketplace/app/virtru\\_data\\_protection\\_for\\_g\\_suite/197076597243](https://gsuite.google.com/marketplace/app/virtru_data_protection_for_g_suite/197076597243)

and add the Chrome extension for automatic decryption and one-click encryption with Gmail

[https://chrome.google.com/webstore/detail/virtru-email-protection-f/nemmanchfojaehgkbgcfmdii\\_dbopakpp?hl=en-US](https://chrome.google.com/webstore/detail/virtru-email-protection-f/nemmanchfojaehgkbgcfmdii_dbopakpp?hl=en-US)

**Know your #1 Vector!**

**#14**

**91%**

The percentage of compromises that occur because of a spear phishing email.

Source: Cofense (previously Phishme) 2016 Study on Enterprise Phishing

**Tip #14:** 9 out of 10 compromises occur through email. Give Email Security the Tender Lovin' Care that it deserves and Elvis intended:

<https://cofense.com/enterprise-phishing-susceptibility-report>

# Hackers Love OOM

## #15

☐ Vacation responder off  
☒ Vacation responder on

First day:  Last day:

Subject:

Message:

Sans Serif

« Plain Text

I am traveling for from August 7th through August 28th. I will be in Costa Rica with Limited Internet Capabilities. In my absence, please contact Bob@MyFirm.com for help!

☐ Only send a response to people in my Contacts

Google Cloud

Proprietary + Confidential

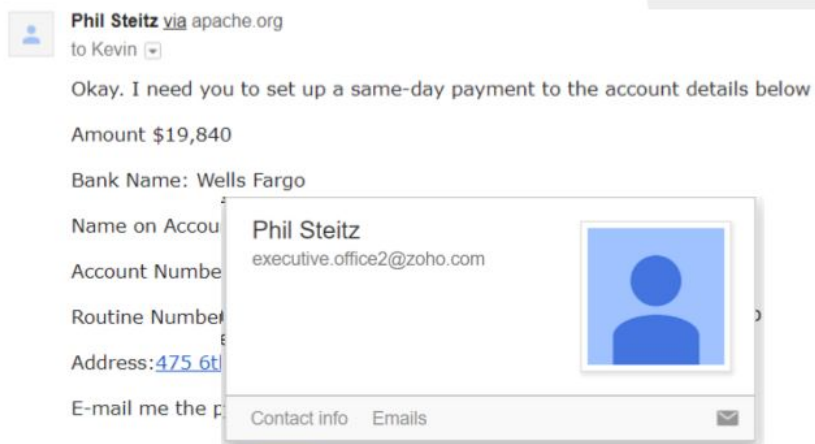
**Tip #15:** Out of Office Messages can be very dangerous. Not only do people tend to over share information but they can be combined with signatures giving tons of contact information!

HINT: Here's what a bad actor sees, "Hi, I am out of the Country. Please come rob my house and feed mittens while you are there! Oh and now is a great time to try and brute force my accounts since I won't get any notices. Plus if you want to impersonate me, now is a good time and here's my contact information in my signature."

If you use Out of Office Messages, make sure you use features like "Only send a response to people in my contacts" or just keep details sparse!

## Watch out for Impersonators!

# #16



**Tip #16:** Bad actors impersonating people and attempting social engineering is a real risk. Money handlers are the number one target.

Above is a real example where the chairman of an organization was spoofed using free emails from zoho.com to try and get a payment made to the account of a money mule.

And while this example is not very elaborate, bad actors can use information from Out of Office messages and social media (more on that in the next 2 tips) for much more convincing attempts.



## Social Media is a Goldmine

Be sensitive about what you post. Birthdays, parents, addresses, pets, graduations, etc. it all adds up! And it's all archived somewhere...



Google Cloud



**Tip #17:** Be sensitive about what information, if any, you post publicly. Nothing on the internet goes away any more and it's trivial to find many people's pictures, birthdates, pet names, parents, home addresses and more. One particularly worrying trend that helps bad actors is the ease of discovering maiden names due to the use of hyphenated last names on Facebook and similar social media platforms.

One urban legend\* I am reminded of is likely from Operation Gold during the cold war. The story goes that the Russian's compromised the operation due to a mole however they did not want to compromise their source. So instead of using phone lines that were tapped for government & military correspondence, they instructed staff to use them for personal calls to keep the enemy busy. The end result is that the intelligence officers monitoring the phones were overwhelmed! Overwhelmed, that is, with personal information that they wouldn't have otherwise had which allowed them to map out personal details like gambling habits, spouses/mistresses, home numbers, relations, etc.

\* anyone have a source for the legend? I've searched to no avail. More photos and information on Operation Gold AKA Operation Stopwatch:

[https://commons.wikimedia.org/wiki/Category:Altglienicke\\_spy\\_tunnel](https://commons.wikimedia.org/wiki/Category:Altglienicke_spy_tunnel)

<https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol-52-no-1/turning-a-cold-war-scheme-into-reality.html>

[http://en.wikipedia.org/wiki/Operation\\_Gold](http://en.wikipedia.org/wiki/Operation_Gold)


# #18

## Business Social Media Spear Phishing

Google


Invitations (4)

Manage all




**Rohit Mishra**

Computer Operator at SAIC

 SAIC


Ignore

Accept




**Dora Shelly**

Sales Manager at SAIC

 SAIC


Ignore

Accept




**Subrata Pandit**

Software Engineer at SAIC

 SAIC


Ignore

Accept



**giakhanh accxi**

Sales Manager at SAIC

 SAIC

Ignore


Accept


See all 4 invitations

Proprietary + Confidential


**Tip #18:** Business Social Media like LinkedIn is a big target as well. Here are several bad actors all impersonating SAIC employees all trying to connect with me.

I've even had a "founder at SAIC" try and reach out to me on LinkedIn. Which is pretty amazing since he died in 2014 at the age of 90 and was named J. Robert Beyster...



Kevin A. McGrail 

Hi Kevin A., I'd like to join your LinkedIn network.



**Jemy Sidons**

Founder at SAIC

Bangladesh

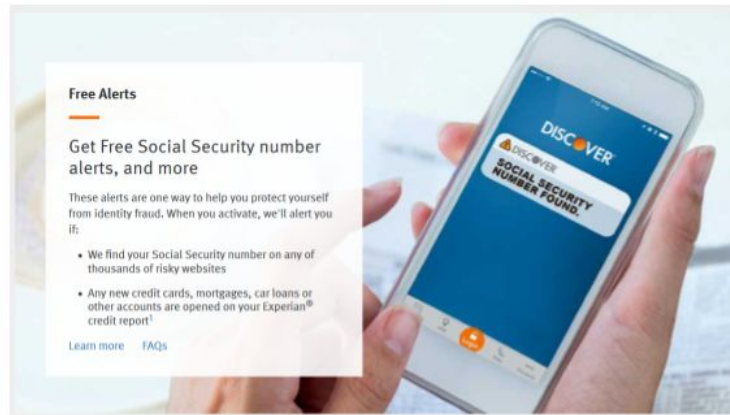
View profile

Accept

## Monitor your Credit

Not a discover member? <https://refer.discover.com/s/pwdup>

#19



Google Cloud

**Tip #19:** Bad guys are typically after money or ways to get money. One way to watch for this is to monitor your personal credit. There are lots of services for this but my recommendation is to sign up for a Discover Card and use their security center. There is no annual fee and there is no extra fee to monitor your FICO score and get SSN / New Account Alerts provided by Experian.

If you sign up at <https://refer.discover.com/s/pwdup>, I get a \$50 credit which goes to the McGrail Foundation, a 501(c)(3) where we “facilitate and advocate for the study, development, creation and distribution of open source, private and secure data communications.”

Plus PwdUp sounds like a security superhero catch phrase, “Password Up, Netizens!”

#20

## Embrace New Ideas!



...before users do so  
outside your control...

Google Cloud

**Tip #20:** This a tip I've learned the hard way. Except in the most controlled environments, Users will just use the tools they want with their own personal accounts. And when they do that, you've lost complete control.

So while you may agree with Dennis Huges or Bruce Schneier that "the only secure computer is one that's unplugged, locked in a safe, and buried 20 feet under the ground in a secret location... and I'm not even too sure about that one", there is always a need to have good balance between security and usability.

## Keep Calm and Have an Incident Response Plan

### KEY GOALS:

Limit damage / Reduce recovery time /  
Lower costs

Speed matters

Key phone numbers / account numbers /  
credentials / list of privileged accounts

Asset Inventory

Paper and Electronic Copies of the Plan

# #21



Google Cloud

**Tip #21:** I'm not saying you need to have a full computer security incident response team (CSIRT) on call but have a basic plan for real-world issues: Successful Phishing Attack, Unauthorized Equipment Found on Network, CryptoWare, Fire/Weather Incident, Lost Equipment, Compromised Account, etc.

Even a basic framework of who to call can help bring some calm to an otherwise bad situation.

Focus on how to limit damage, keep costs under control and recover in the shortest time.

And in most of these incidents, speed matters. Your CEO leaves his phone in a public place. Can you remote lock it? Do you need to remote wipe it? What's your policy? How can you issue him a new phone and transfer his number?

And it's important to keep a list of key phone numbers / account numbers / credentials / list of privileged accounts. Do you have an inventory of assets and their location?

And once you have these items, make sure you have Paper and Electronic copies! Don't get caught in a Catch-22 where you need passwords and instructions only stored on a system to restore the system.

Good incident response planning is the difference between being a hero or a zero when a problem arises! And while I'd like to stress a lot on testing your plans, I'll settle for at least having something in writing with a commitment to revise the plans after each incident.

# #22

## Monitor

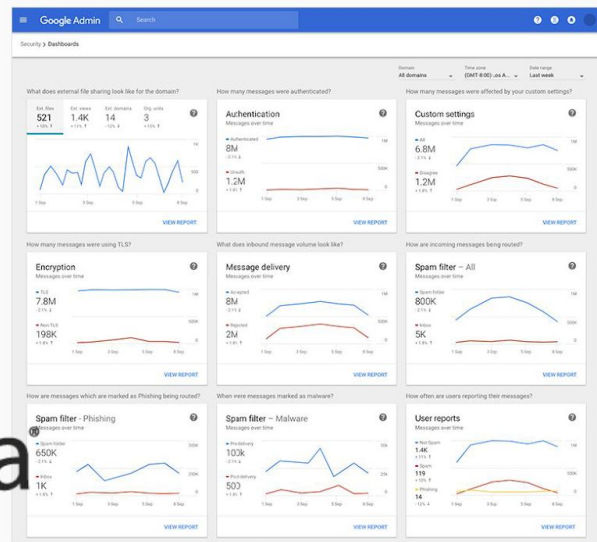
I like to know about issues before my users. Tools like Google's Security Center Dashboard (Enterprise Edition only) and AppNeta can help.

Use the Dashboard to know which users are being targeted for phishing!



# AppNeta

Google Cloud



Proprietary + Confidential

**Tip #22:** I want to know about a problem before my users even know there is a problem.

If you are Enterprise Edition, the Google Security Center Dashboard is an excellent resource. One useful technique is to use it for information on which users are being targeted by bad actors. Know your vectors!

Also, two must have links are:

G Suite App Status: <https://www.google.com/appsstatus#hl=en&v=status>  
&

Cloud Connect Community: <https://www.cloudconnectcommunity.com/ccf/>

NOTE: The Cloud Connect Community routinely identifies outages before they are posted on the App Status page.

And I love commercial tools like AppNeta and Pingdom.

# #23



## Explain “Why?”

Or just use Cunningham’s law...

Google Cloud



**Tip #23:** Show users some of the “why” without scaring them.

Every user is a target if only from automated, brute force attacks. Show them reports from things like haveibeenpwned.com.

And users love things like 2SV \*after\* they’ve been compromised...Talk to them about Google’s Zero compromised accounts statistics.

Using Mobile Device Management? Show them you can remote wipe a phone and it’s just a piece of hardware that can be replaced.

Otherwise tell them the wrong reason and hope that Cunningham’s Law works!

*“The best way to get the right answer on the internet is not to ask a question; it’s to post the wrong answer.”* - [https://meta.wikimedia.org/wiki/Cunningham%27s\\_Law](https://meta.wikimedia.org/wiki/Cunningham%27s_Law)



## Quis Custodiet Ipsos Custodes?

USENIX / Systems Administrator's Code of Ethics

<https://www.usenix.org/system-administrators-code-ethics>



# #24

**Tip #24:** Who will guard the guards themselves?

As a member of the Large Install System Administration (LISA) group (formerly [sage]), I'm proud to follow the LISA Code of Ethics. This document, co-signed by LOPSA, USENIX, and LISA, is something I refer to as the "IT Ten Commandments" and I strive to make sure every administrator follow it in everything that we do.

I strongly recommend every computer IT professional adopt this code.

<https://www.usenix.org/system-administrators-code-ethics>



## Sage Advice from a Founding Father

If you aren't paying for it, you ARE the product.

Too good to be true? It probably is...



#25

Google Cloud

**Tip #25:** OK, Ben Franklin probably didn't say these but I like to think he would agree with the sentiment.

Many scams can be quickly interrupted by asking yourself the question of whether it's too good to be true. If it's yes, sit on it for a few days and ask some security people for advice. Nigerian princes are not donating their gold to needy people, Western Union is not holding a transfer for you, Microsoft is not calling you to help you with your computer and the IRS does not take payment with Walmart gift cards.

So how is Gmail (not G Suite) free? It's free because you are the product. Advertising and data mining supported business models are a legitimate reality and one that can be a win-win relationship if you understand what you and they are doing.

Over the Air Television is free in the US because it is an advertising supported revenue model. Some prefer to pay for streaming services like Netflix instead which has no advertising. Both are legitimate business models.

In this day and age, barely a week goes by without a privacy concern with your data so think carefully about the services you use and the companies you trust!

## “Invoice” Scams

“This notice is not a bill...”

Pay no attention to the man  
behind the curtain...

#26

**iDNS**  
Internet Domain Name Services

Domain Name Expiration Notice  
WEB 08-27-2018 www.idns.net

As a courtesy to domain name holders, we are sending you this notification of the domain name registration that is due to expire in the next few months. When you switch today to Internet Domain Name Services, you can take advantage of our best savings. Your registration for [REDACTED] will expire on December 4, 2018. Act today!

Domain name: [REDACTED]  
Reply Requested By: September 24, 2018

You must renew your domain name to retain exclusive rights to it on the Web, and now is the time to transfer and renew your name from your current Registrar to Internet Domain Name Services. Failure to renew your domain name by the expiration date may result in a loss of your online identity making it difficult for your customers and friends to locate you on the Web.

Privatization of Domain Registrations and Renewals now allows the consumer the choice of Registrar when initially registering and also when renewing a domain name. Domain name holders are **not obligated to renew their domain name with their current Registrar or with Internet Domain Name Services.** Review our prices and decide for yourself. You are under no obligation to pay the amounts stated below, unless you accept this offer. This notice is not a bill, it is rather an easy means of payment should you decide to switch your domain name registration to Internet Domain Name Services.

Term	Period covered	Price
1 year	Until - Dec 4, 2018	\$43.00
2 years (Recommended)	Until - Dec 4, 2020	\$80.00 (save \$10)
5 years (Best Value)	Until - Dec 4, 2023	\$180.00 (save \$40)

The following names are currently available for you to register and secure, protecting your domain name from being duplicated.

Available Domain	Period covered	Price
[REDACTED]	2 Years	\$80.00
[REDACTED]	2 Years	\$80.00

For a complete list of our terms and conditions, please visit [www.idns.net](http://www.idns.net)

Transfer and renew your domain name online at [www.idns.net](http://www.idns.net) 24 hours a day, 7 days a week.

Please detach this card and include it with your payment.  
Check the appropriate boxes of the Domain Name(s) you would like to order.

Expiration Date	Reply Requested By	Renewal Term	Payment
December 4, 2018	September 24, 2018	1 Year	\$43.00
		2 Year	\$80.00
		5 Year	\$180.00

Total Amount: [REDACTED]

If paying by credit card, please enter your information below:  
Card Number: [REDACTED]  
Expiry: [REDACTED]

Please provide a valid email address on the above line

## “Invoice” Scams

“This is an advertisement...”

**Warn your A/P. We see  
more than a few of these  
get paid!**

#26

Warranty Services  
Extended Coverage Department

Owner ID #: CE-9086311  
Contact Phone: 1-877-324-0916  
Vehicle Make: HONDA, NISSAN, TOYOTA  
Program Term Deadline: 7/3/2018  
Call to verify the above information  
Read below for more information

**IMMEDIATE RESPONSE TO THIS NOTICE REQUESTED**

\*\*\*\*\*AUTOMOTIVE S-DIGIT 22001  
[REDACTED]

**IMMEDIATE RESPONSE TO THIS NOTICE REQUESTED**

Owner ID #: CE-9086311  
Coverage Status: AVAILABLE  
Program Term Deadline: 7/3/2018

Make: HONDA, NISSAN, TOYOTA  
Attention: Mr. McGeal

Our records indicate that you have not contacted us to have the vehicle service contract for your HONDA, NISSAN, TOYOTA Updated. You are requesting this notice to ensure no lapse in warranty coverage. Warranty expiration is based on the mileage and age of your HONDA, NISSAN, TOYOTA Call now to update your coverage.

Please Call: 1-877-324-0916 Para Espanol: 1-877-282-9764

By neglecting to replace your coverage you will be at risk or being financially liable for any and all repairs after your factory warranty expires. However, you still have time left to activate your service contract on vehicle before it's too late. No vehicle inspection will be required.

Your file on this vehicle will be deleted and you may no longer be eligible for this offer regarding service coverage after 7/3/2018.

Personalized Website: <http://CE-9086311.automotiveworks.info>

SUMMARY OF TERMS							
APR	1.5%	2.75%	3.75%	4.5%	5.85%	9.25%	11.99%
APPROVED	N/A	N/A	N/A	N/A	N/A	N/A	N/A

Coverage Expiration	Platinum Option: Engine, Transmission, Transfer Unit of 6x4, Drive Axle Assembly, Front End and Rear Suspension, Steering, Air Conditioning Unit, Electronics, Seats, Gauges, Brake System, and Most mechanical Parts.
1. EXTENSION THROUGH 2023	
2. UP TO OR AN ADDITIONAL 100K MILES	
3. PLATINUM POWERTRAIN	

PHONE: 1-877-324-0916 Call No Later Than: 7/3/2018

Operating Hours: Monday - Friday 8:00am to 7:00pm CST & Saturday 9:00am - 2:00pm CST

**Tip #26:** This tip is fairly basic. There are a number of invoice scams that revolve around sending advertisements that look a lot like bills. Warn your accounts payable departments to watch out for these! In the fine print, they typically have something that indicates they are not an invoice!

# Offboarding

Make sure exiting employees have their accounts disabled!

# EXIT

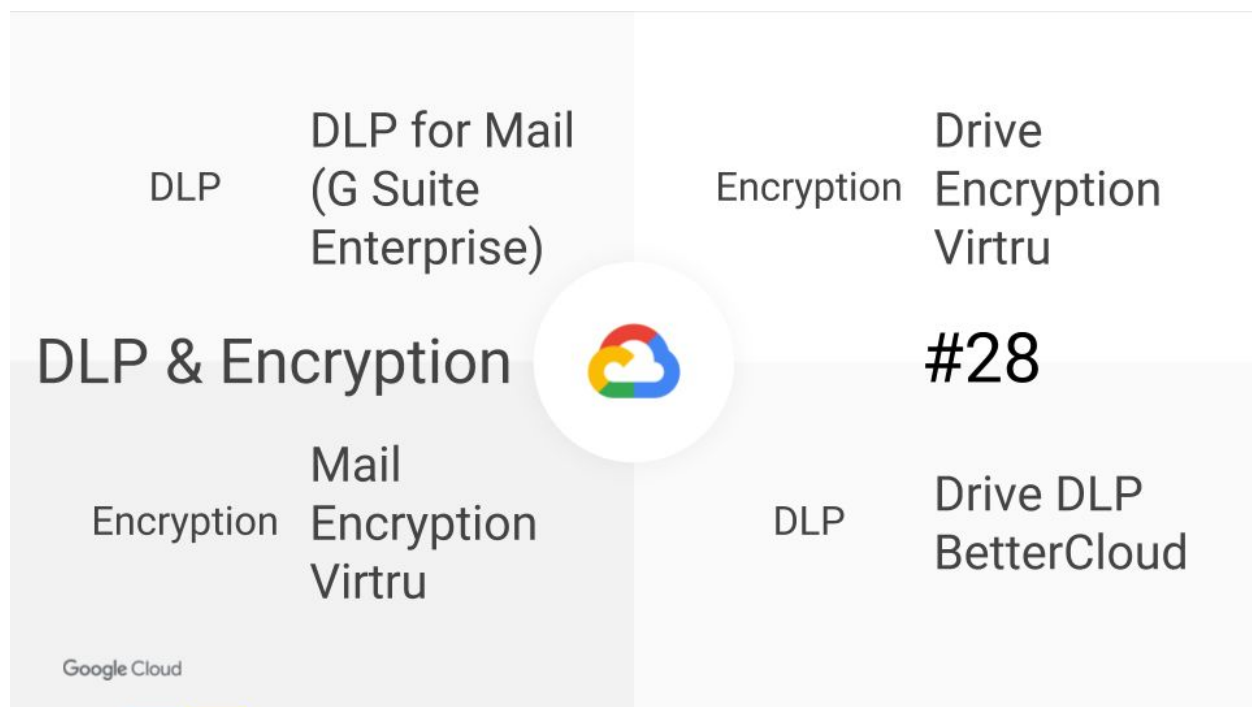
#27

 BetterCloud

Google Cloud

**Tip #27:** Make sure you have a clear process for offboarding employees. Don't leave accounts active after an employee exits. And just changing the password won't revoke access for programs with API access or a less secure application password!

Tools like BetterCloud can make you more secure by automating the process and save you money by making sure your cloud licenses are recouped.



**Tip #28:** Data Loss Protection and Encryption are essential in preventing damaging data loss.

If you are a G Suite Enterprise customer, DLP for Mail is included with tools like a DLP Predefined Content Detector for regular expression testing and geolocale specific rules.

And the combination of DLP and Encryption in Virtru for Email can educate users what they should encrypt by identifying issues such as Tax IDs in email and prompting for encryption.

BetterCloud also provides DLP for Drive with both one time audits and real-time policies.

Finally, just announced at NEXT, Virtru is now Google's only Data Protection Partner and Encryption for Drive is coming this year:

<https://techcrunch.com/2018/07/25/virtu-teams-up-with-google-to-bring-its-end-to-end-encryption-service-to-google-drive/>

## Turn on Your Alerts

Starting to rollout on August 1, Google is adding Government backed attacks to the Alerts you can manage.

Make sure you review your alerts:  
*"Admin Console > Reports > Manage Alerts"*

# #29

**Tip #29:** Google G Suite provides a number of alerts. Make sure you review your settings and turn them on! Navigate to the Admin Console at [admin.google.com](https://admin.google.com) and go to Reports > Manage > Alerts. New alerts like the Government backed attack alert are disabled by default.

**Trick of the Day:** The power button for the Pixelbook is a built-in U2F security key.



chromebook

“The Chromebook is a real challenge;  
full encryption and cheap.  
The two worst fears for security and  
digital forensics.”

Amber Schroader

*Paraben Corporation*



#30

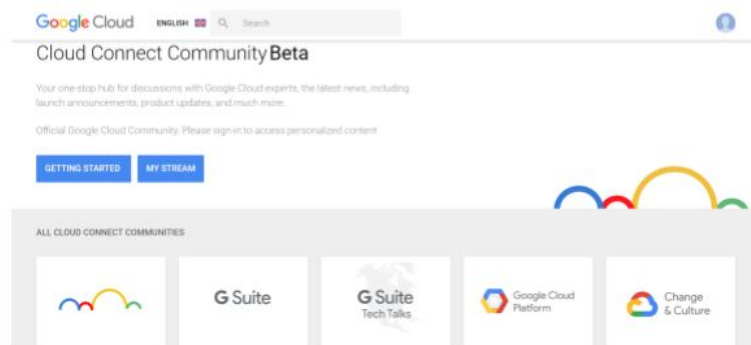


**Tip #30:** Chromebooks come in all flavors, sizes and costs from \$100 to \$1800 but one thing remains the same. They are unbelievably secure and when combined with device management and a security key, they are without a doubt the most secure system available today.

And as my final trick for today, the pixelbook has a U2F security key built in. See <https://9to5google.com/2018/06/08/pixelbook-power-button-u2f-security-key/> for more information!

# Join the CCC

# #31



**Tip #31:** This is a bonus tip with two parts. First, join the Google Cloud Connect Community (CCC). Second, learn from others on the CCC.

Point in case, something I learned recently from others was posted by Steve Larsen on the CCC<sup>1</sup>. His trick lets you have complete separation of privileges for your day to day account for all your admins without spending money on an extra license.

This lets you increase the security of your SuperAdmins and you can do so without incurring a license cost by using Google's Cloud Identity Free licenses. This is the security principle called "Least Privilege".

To do so, first navigate to the Admin Console via [admin.google.com](https://admin.google.com) and go to Billing. Once there, activate the Cloud Identity Free product. After you do this, you'll want to turn off Automatic License assignment for your G Suite product billing.

Now you can create users and assign the SuperAdmin role without using a G Suite license. And as Jack Woodward comments, you can use G Suite address mapping to map the email address to another email account.

NOTE: You'll need to remember to assign a G Suite product license to new users that you want to have a license.

---

<sup>1</sup> <https://www.cloudconnectcommunity.com/ccc>

Author: Kevin A. McGrail

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

## Photo Credits:

XKCD comics CC BY-NC 2.5 from <https://xkcd.com/936/> & <https://xkcd.com/1820/> - <https://creativecommons.org/licenses/by-nc/2.5/>

KAM photo taken by Ted King, used with permission.

Rings Photo by FOX from Pexels.com

Angela Merkel Photo from Bundesregierung/Kugler

Chain Photo by Miguel Á. Padriñán from Pexels.com

Operation Gold Bundesarchiv, Bild 183-37695-0003 / Junge, Peter Heinz / CC-BY-SA 3.0 - <https://creativecommons.org/licenses/by-sa/3.0/us/> - Added Twitter logo as a satire on a 1956 photo for juxtaposition - The image "Slide 17" is licensed CC-BY-SA 3.0 as well.

Facebook & Twitter Logos Brand Resources of their Respective Companies

Lightbulb image by Pixabay CC0 License - <https://creativecommons.org/share-your-work/public-domain/cc0/>

Keep Calm Poster, Obverse of \$100 Bill, Ben Franklin Signature & Exit Sign from Public Domain

Security Code Fail taken by Xavier Mertens, used with permission

Copyright © 2018, The McGrail Foundation, All Rights Reserved.  
Licensed under CC BY-NC 4.0: <https://creativecommons.org/licenses/by-nc/4.0/>