



Using LinkedIn for **Raising Security Awareness**

Session 3: Content Creation



Homework Check :)

✓ **Post** 2-3x this week!

✓ **Engage** with your audience

✓ **Apply 2 format** tips to your post

✓ **Follow** 3 'thought leaders' who resonate with you

✓ **Post** 2-3x this week!

- ☐ Curate one piece w/YOUR insights
- ☐ Post with a picture
- ☐ Repurpose SA messaging





Getting Started



Consider Audience

- ▶ Regular Users (aka Employees)
- ▶ Cyber Peers (Internal IT & Security, External Networking/Professional Branding)
- ▶ Leadership (Directors, Exec Team, Board)



AAA Strategy

Richard van der Blom

- ▶ **Authentic** (Personal stories = Relatable; Opinions = Expertise/Thought Leadership)
- ▶ **Active** (Industry News = Informed & Current; Engage with Network = Relationship Building)
- ▶ **Approachable** (Respond to Messages; Proactively Reach Out)



Regular Users/Employees

▶▶▶ Educate

▶▶▶ Repurpose internal content for awareness

▶▶▶ Share what HR won't allow on internal comms



Suggested content types: Blogs, Videos, Infographics, Explainers, Guides



Gabriel Friedlander • 1st

Wizer - Free Security Awareness Training | Founder

1w • 🌐

Share this with your kids and Stay Wizer Online!

— wizer —

10 Internet Safety Rules To Discuss With Your Kids Now

wizer-training.com



Stephen Smith and 178 others

12 comments • 72 reposts



Gabriel Friedlander • 1st

Wizer - Free Security Awareness Training | Founder

1w • 🌐

Share this with your kids and Stay Wizer Online!

— wizer —

1

DON'T DOWNLOAD FREE GAME CHEATS OR TOKENS

We Share the Same WiFi, You Will
Get Us All Infected!



Stephen Smith and 178 others

12 comments • 72 reposts

OPENING SLIDE

(what's the hook?)



XX%

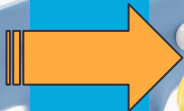
Fun fact you want to
Highlight put it in here



SCREENSHOT IN HERE

Start your
image on **one**
slide, copy the
box and
continue it on
the next slide.

➡ LIKE THIS



➡ SEE how
cool is this?



END SLIDE

(Give a Call-to-action)

ZOECIAL
MEDIA

Examples



Tom Smith III • 1st

Protecting you from danger online by teaching you about cybersecurity // H...
1mo • 🌐

The most secure people don't spend a fortune on cybersecurity.

They get the basics right.

Do these things and you you'll be more secure than most:

- Use antivirus software.
- Have current backups that you've tested recovering from.
- Use a password manager.
- Have unique passwords for every login.
- Enable MFA everywhere you can.
- Keep your devices and software up to date, including your home network.
- Security awareness training is essential.

There are other things you can do to be more secure, but if you do these you'll be way ahead of most people.

Which of these is the most difficult for you?

🌐 You and 8 others

5 comments



Heather Noggle • 1st

Translating between English and Tech | Connecting people and systems | 🌐 Cyb...
3d • 🌐

There were mice in the house. And I just learned this yesterday.

Evidently, I don't know much about country living. Even after the numerous skinks and 3 or 4 (known) snakes we've found lurking in the basement - lots of spiders... It was the mice that got me.

Mice! We have cats (more numerous than snakes) - why mice?

We used to keep the cat food in a lower cabinet under the downstairs sink. We stopped because the mice were getting it. With the cabinet door there and them secured behind it - and some stealth, the mice nibbled at the cat food, and the cats were oblivious to their entry and theft.

The nerve! Improper access!

Now the cat food goes in an upper cabinet, secured where neither cats nor mice may nibble.

The cat food is, of course, the crown jewels of our storied conversation.

Secured properly, it's of maximum utility and at maximum safety. It's the prize.

Mice do what mice do. Cats do what cats do. Their behavior's somewhat predictable, and with predictable behavior, our defense goes more smoothly.

Personify cyberattackers. What do they seek? Why? What do you have to protect? How?

The wrong way to detect the cat food breach is to find a nibbled-through bag and missing food. But at least that's obvious. Its cyber equivalent...not always immediately.

You can guess the cat food brand...because it's just too funny. IAMS.

Mice will play. (It wasn't even cheese flavored)

Enjoy the rest of your weekend.

[#cybersecurity](#) [#catandmouse](#) [#countryliving](#) [#IAM](#)

Be a Rebel

Wizer *Stories*

How I Was Blackmailed

Based on a True Story

© Wizer Inc.



Wizer

Deep Fake Job Scam



Wizer *Stories*


I LOVED Him But He Scammed Me

Based on a True Story

© Wizer Inc.



Examples



Gabriel Friedlander • 1st
Wizer - Free Security Awareness Training | Founder
1d • 🌐

...

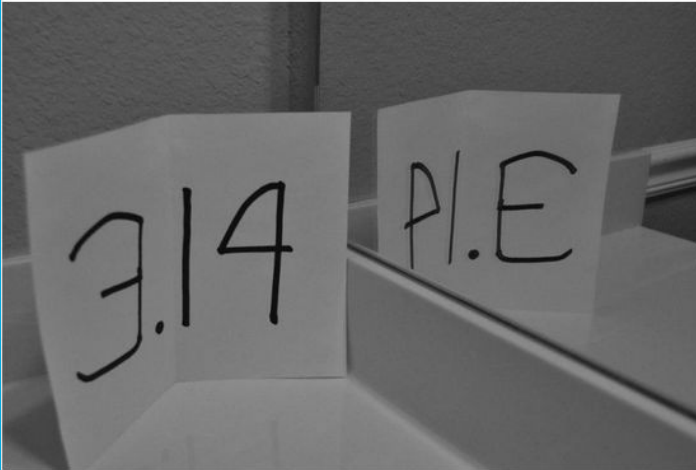
Today is Pie Day and I have a nerdy question for all of you :) Because Pi is an infinity sudo random number, you can probably find all our bank accounts in it. If that's the case, are pie pointers considered PII data?




Also:

Pie day is today - March 14th
Stephen Hawking died on March 14th
Albert Einstein was born on March 14th
They were both 76 when they died...

And 3.14 in the mirror is 🍷

That's all I have today about pie 😊



   Stephen Smith and 69 others

10 comments · 7 reposts





Cyber Peers



Professional Insights



Industry Validation Audience Readership, Analysts, Journalists - TAG THEM







Geek Out

Suggested content types: Current News, Industry Reports, Infographics, Polls, LI
Lives, Case Studies, Webinars, Whitepapers



Examples




 **Graham Cluley** • 1st
Cybersecurity expert, host of "Smashing Security" podcast, public speaker. Needs hai...
1mo • 



Reddit has been hacked. Attackers gained access to:

- * internal documents
- * code
- * some internal business systems.

Reddit believes, at the moment, that users' passwords and accounts are safe.



r/reddit on Reddit: We had a security incident. Here's what we know.
reddit.com • 3 min read

  Melissa Chaney, MBA and 513 others

30 comments • 128 reposts



Gal Helemski • 2nd
Co-Founder & CTO/CPO at PlainID
1yr •

+ Follow ...

"Role-based access control is crucial for agencies' cybersecurity as the federal government shifts to a more distributed and hybrid workforce" - even the subtitle to this article makes me frightened for federal organizations considering RBAC as the correct authorization management system to use.

RBAC has been around for a long time and it is very commonly used, but that does not make it the most trusted solution to use.

While I agree that RBAC is based on a very simple design which could be the attraction here, it also means rigidity in the way it works.

RBAC can't be amended quickly in emergencies and it can't grant permissions based on time or location.

And probably the most important point that federal agencies are overlooking is that as organizations grow and more roles are added or when people change roles, users are left with unnecessary permissions, increasing risk exposure.

Jay Bretzmann, IDC's Program Director points out 2 things:

- Roles change pretty frequently, and organizations can end up with hundreds of definitions — a lot of them obsolete and a security vulnerability when they aren't deleted.
- Effective RBAC implementation requires a cyclical approach that sees organizations continually defining and redefining roles to ensure access frameworks match the reality of remote and hybrid operations while simultaneously limiting total risk.

Essentially RBAC is high maintenance! Do federal agencies have the time and resources to implement these time-consuming extra steps? I think not.

There is another way... Policy-based Access Control!

#PBAC supports environmental and contextual controls, policies can be adjusted quickly and give access for set periods of time, groups of users can be added, removed, or amended with ease and obsolete permissions revoked with a click. All this creates a more secure and flexible system that does not expose agencies to unnecessary risk and it does not undermine Zero Trust objectives that even the White House is working towards.



The Principle of Least Privilege in Federal Agencies: Implementing RBAC

fedtechmagazine.com • 4 min read

Haidee LeClair and 27 others

6 comments



Gemma Goldstein • 1st

Head of Inbound at Envy | B2B SEO, Social Media, Strategy, Content and oh so much...
6mo • 🌐

Key takeaways from [Google #SearchOn](#):

- 1) Already searching with text is indispensable, but now the age of visual search is here. Your camera is the next keyboard - Lens is used 8 billion times a month, but is it really for B2B?
- 2) Multisearch is coming to 70 languages this autumn - combining images and text. It even includes multisearch near me. Still not sounding so relevant for B2B.
- 3) As people start typing a question google will suggest questions and offer images and descriptions below, reviews and more. They will allow you to select topics to expand or refine your search
- 4) People engage with 3d models 50% more than 2d
- 5) Page insights- when you are on a webpage on your phone Google will pop up with related content and more information about the site you are on
- 6) ALL examples were given on phones indicating Google sees search going completely mobile

Overall there were many advances in the B2C search realm and less in the B2B, but these impacts will creep over into B2B soon enough....

Thanks [Prabhakar Raghavan](#), [Dounia Berrada](#), Yvonne Wei Chou, [Nick Bell](#), Sophia Lin, [Lilian Rincon](#), Yul Kwon, [Christopher Phillips](#), [Hema Budaraju](#), [Rubén Lozano Aguilera](#)

[#SEO](#) [#Content](#) [#GoogleSearch](#)

My key takeaways
from [Google](#)
#SearchOn 2022

1

Already searching
with text is
indispensable, but
now the age of visual
search is here.



Your camera is the
next keyboard - Lens
is used 8 billion times a month, but is it really for B2B?

2

Multisearch is coming
to 70 languages this
autumn - combining
images and text.

Video!

▶ Video Editors

Veed

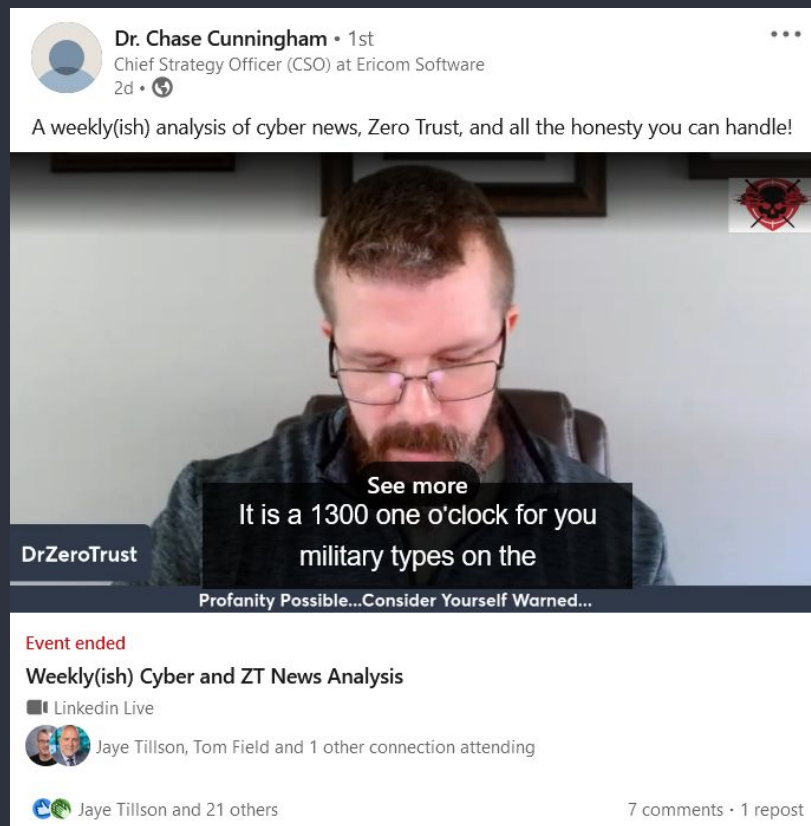
Descript

Peech

▶ Video Livestream

Streamyard

Restream



The screenshot shows a LinkedIn post from Dr. Chase Cunningham, Chief Strategy Officer (CSO) at Ericom Software. The post is a live stream titled "Weekly(ish) Cyber and ZT News Analysis". The video shows Dr. Cunningham speaking, with a redacted area containing the text "It is a 1300 one o'clock for you military types on the". Below the video, the text "Profanity Possible...Consider Yourself Warned..." is visible. The post has 7 comments and 1 repost.

Dr. Chase Cunningham • 1st
Chief Strategy Officer (CSO) at Ericom Software
2d •

A weekly(ish) analysis of cyber news, Zero Trust, and all the honesty you can handle!


See more
It is a 1300 one o'clock for you
military types on the

DrZeroTrust

Profanity Possible...Consider Yourself Warned...

Event ended
Weekly(ish) Cyber and ZT News Analysis
LinkedIn Live
Jaye Tillson, Tom Field and 1 other connection attending
Jaye Tillson and 21 others
7 comments • 1 repost

Video-in-the-Raw

**Stephen Semmelroth** • 1st
Leader
8mo • 🔒

COUNT THEM: NINE NEW ENGINEERING #QuickHits in the AVANT Communications #Pathfinder today!

- 🏠 CCaaS Integrations with [Chris Brennan](#)
- 🏠 Reputation Management with [John Paullin](#)
- 🏠 Win Every Colo Deal with [Chip Hoisington](#)
- 🏠 Benefits of an Aggregator with [James Christian](#)
- 🏠 Telecom Basics with [Peter Callowhill](#)
- 🏠 The Business of Ransomware: Conti with 🔥 [Stephen Semmelroth](#)
- 🏠 UCaaS Verticals with [John Paullin](#)
- 🏠 Strategic Enterprise Selling with [Brent Wilford](#)
- 🏠 Solving People Problems - Staffing and Recruiting with 🔥 [Stephen Semmelroth](#)





Leadership

▶▶▶▶▶ Content Overlap of Employee Education + Cyber Insights

▶▶▶▶▶ Education as Individual (aka Employee content is still highly relevant)

▶▶▶▶▶ Industry Insights from Cyber View

Suggested content types: Blogs, Videos, Infographics, Explainers, Guides



Targeted Content

- ▶ Break down concepts from industry reports
- ▶ Repurpose into other formats: video, slides, infographic, memes



Batch & Create Themes



March 2023					KEY:	
2023-03-13	2023-03-14	2023-03-15	2023-03-16	2023-03-17	Theme 1	Romance scams
					Theme 2	Rising use of AI
					Theme 3	Job Scams
2023-03-20	2023-03-21	2023-03-22	2023-03-23	2023-03-24	Theme 4	Impact on Company and friends
					Theme 5	Rise in trust in social platforms
2023-03-27	2023-03-28	2023-03-29	2023-03-30	2023-03-31	Theme 6	Relaxed mode vs. alert mode
					Theme 7	Connections and Integrations
2023-04-03	2023-04-04	2023-04-05	2023-04-06	2023-04-07		
2023-04-10	2023-04-11	2023-04-12	2023-04-13	2023-04-14		
2023-04-17	2023-04-18	2023-04-19	2023-04-20	2023-04-21		
2023-04-24	2023-04-25	2023-04-26	2023-04-27	2023-04-28		

► *Maximize planning, minimize time*

Prompts for ChatGPT/AI



Cyber tips can get old BUT we can change up HOW we present them

1. What would I not think about [this]
2. What is unknown or less common answers questions about
3. Give me something original about this topic that some people believe to be untrue
4. Write some potential ideas for increasing security awareness
5. Expand on number X
6. Write a 1-minute video script for commercial about strong passwords
7. Make it funny
8. Rewrite the first line to be witty / hook
9. Top 10 things
10. What are the key takeaways from this
11. Top 5 famous quotes about
12. Write a poem/fairytale/song





#HashtagReview

- ▶ Sweet spot is 3-5
- ▶ Not all #s are created equal
- ▶ Use a mix of broad and niche #s



Hashtags for Audience

Employee		Peers		Leadership	
#family	23K	#phishing	10.4K	#databreach	11.1K
#kids	3.3K	#securityawareness	16K	#CEO	80.7K
#onlinesafety	409	#securityawarenesstraining	500	#SaaS	26K
#jobhunting	28K	#GRC	4.9K	#Healthcare	9.6M
#jobhuntingtips	1.2K	#cybersecurity	573K	#oilandgas	327K
#smallbusiness	813K	#privacy	510K	#enivronment	122K

Get Inspired By Cyber Peers

[Danny Pehar](#)

[Naomi Buckwalter](#)

[Gabriel Friedlander](#)

[Heather Noggle](#)

[Jax Scott](#)

[Joanna Udo](#)

[Jane Frankland](#)

[Stephen Semmelroth](#)

[Maril Vernon](#)

[Mike Miller](#)

[Chris Roberts](#)

[Anastasia Edwards](#)

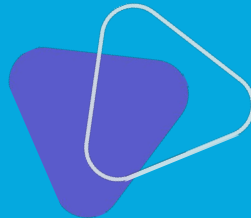
[Neal Bridges](#)

[AJ Yawn](#)

[Sarah Armstrong-Smith](#)

[Gerald Auger](#)

[Jay Jay Davey](#)



Learn from Social Media Rockstars



Gemma Goldstein - Social Media, Strategy, and Content

Zoe Bermant - CEO Zoecial Media

Aliza Hughes - Director of Thought Leadership, Zoecial Media

Shari Wright - Pilo - Digital Marketing Consultant, Educator, Canva Champion

Richard van der Blom - LinkedIn & Social Selling Trainer



SAM Community!

Weekly Virtual Meetups

Bi-Monthly Livestreams

Security Awareness Resources

Get our email updates:
wizer-training.com/manager-hub