



# Cyber Security Awareness







```
for i in people.data.users:
    response = client.api.statuses.user_timeline.get(screen_name=i.scre
    print 'Got', len(response.data), 'tweets from', i.screen_name
    if len(response.data) != 0:
        ltdate = response.data[0]['created_at']
        ltdate2 = datetime.strptime(ltdate, '%a %b %d %H:%M:%S +0000 %Y
        today = datetime.now()
        howlong = (today-ltdate2).days
        if howlong < daywindow:
            print i.screen_name, 'has tweeted in the past' , daywin
            totaltweets += len(response.data)
            for j in response.data:
                if j.entities.urls:
                    for k in j.entities.urls:
                        newurl = k['expanded_url']
                        urlset.add((newurl, j.user.scre
            print i.screen_name, 'has not tweeted'
```

The Cyber Security we  
are talking about today  
does NOT look like this





The image features a central, dark blue, irregularly shaped graphic that resembles a splatter or a cloud of paint. The graphic has a textured, slightly grainy appearance and is surrounded by a lighter blue, splattered background. The text "Most Hacking Is Low-Tech" is centered within the dark blue area in a white, sans-serif font. The overall composition is clean and modern, with a focus on the text and the abstract background.

Most Hacking  
Is Low-Tech

# Social Engineering

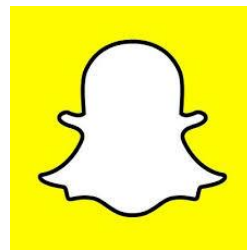
- The manipulation of the natural human tendency to trust
- Social Media
- Email
- Phone
- On-Site



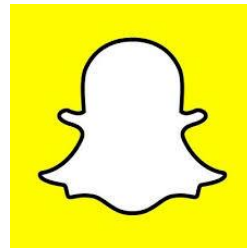


# Socially Acceptable....

- Family Info
- Vacations & Travel
- Likes & Dislikes
- Friends & Pets
- Places Lived
- Causes Supported



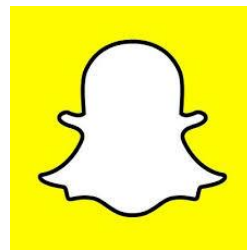
Socially Acceptable....





Socially Acceptable....

## EXAMPLES



Ain't nobody **crazier**  
than your cousins on  
your mama side



#ijs

# birthday scenario

## THE AVENGERS VERSION

- |                               |                                |                            |
|-------------------------------|--------------------------------|----------------------------|
| 1. went clubbing with         | 17. wrecking havoc with        | <b>JAN</b> THOR            |
| 2. best friends with          | 18. got trolled by             | <b>FEB</b> IRON MAN        |
| 3. being stalked by           | 19. is actually the child of   | <b>MAR</b> ERIK SELVIG     |
| 4. ruling over humans with    | 20. first kiss stolen by       | <b>APR</b> BLACK WIDOW     |
| 5. gained the powers of       | 21. isolated on an island with | <b>MAY</b> THE CHITAUURI   |
| 6. had babies with            | 22. shared an ice cream with   | <b>JUN</b> HAWKEYE         |
| 7. got into a fight with      | 23. is actually a sibling of   | <b>JUL</b> PHIL COULSON    |
| 8. swapped personalities with | 24. got kidnapped by           | <b>AUG</b> LOKI            |
| 9. went on a date with        | 25. bound for life to          | <b>SEP</b> NICK FURY       |
| 10. formed a team with        | 26. started a company with     | <b>OCT</b> BRUCE BANNER    |
| 11. formed a band with        | 27. crashed a party with       | <b>NOV</b> THE HULK        |
| 12. is worshipped by          | 28. went to the beach with     | <b>DEC</b> CAPTAIN AMERICA |
| 13. showered together with    | 29. went to prom with          |                            |
| 14. saved the world with      | 30. is hugging                 |                            |
| 15. became the sidekick of    | 31. created a new world with   |                            |
| 16. became the boss of        |                                |                            |



**TYPE “HALLOWEEN” AND  
THE YEAR YOU WERE  
BORN IN THE GIF BAR.**

**THATS YOUR COSTUME  
THIS YEAR...**



Somebody, please play. I want to see your answers:

- \* How old are you: 43
- \* Surgeries: 2
- \* Tattoos: 3 i need more
- \* Ever hit a deer: yes
- \* Rode in an ambulance: yes
- \* Ice skated: yes
- \* Rode on a motorcycle: Yes
- \* Stayed in hospital: yes
- \* Skipped school: yes
- \* Last phone call: [REDACTED]
- \* Last text from: [REDACTED]
- \* Watched someone die: yes
- \* Pepsi or Coke: Pepsi
- \* Favorite pie: coconut cream
- \* Favorite pizza: hamburger and green olive
- \* Favorite season: spring
- \* Broken bones: 6 ( 4 ribs, big toe and neck)
- \* Received a ticket: yes
- \* Favorite Color: midnight blue
- \* Sunset or Sunrise: sunrise
- \* Who will play along: a few



Your Movie Star Name

=

Mother's Maiden Name

+

Social Security Number

OMG!

What's Your Movie Star Name?



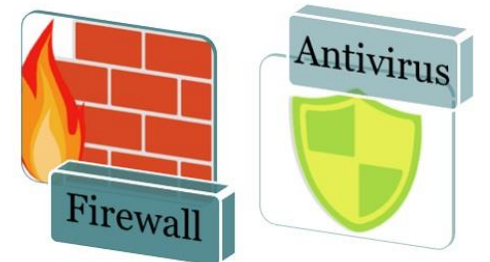
As this information is assembled,  
they are ready to take the next step



- Urgency
- Emotion
- Empathy
- Authority

# Email is the Key to the Network

- Phishing
  - Links & Attachments
  - vv  $\neq$  w
- Business Email Compromise (BEC)
  - Personalized – grammar, signatures, etc



# Can you spot the hack?

**From:** Keith Fotta [<mailto:kfotta@proactivemanagedit.com>]  
**Sent:** Tuesday, March 21, 2017 12:24 PM  
**To:** Lori Sacchetti <[lsacchetti@purechannelit.com](mailto:lsacchetti@purechannelit.com)>  
**Subject:** Payment.

Pay the attached invoice, payment is for a Legal/Professional Fees.

Cheers,  
Keith



**Keith Fotta**  
*Chief Executive Officer*  
**Pro-Active Managed IT™**

W | +1 (652) 379-2025  
C | +1 (617) 398-0070  
E | [kfotta@proactivemanagedit.com](mailto:kfotta@proactivemanagedit.com)  
[www.proactivemanagedit.com](http://www.proactivemanagedit.com)



**From:** Keith Fotta [<mailto:kfotta@proactivermanagedit.com>]

**Sent:** Tuesday, March 21, 2017 12:24 PM

**To:** Lori Sacchetti <[lsacchetti@purechannelit.com](mailto:lsacchetti@purechannelit.com)>

**Subject:** Payment.

Pay the attached invoice, payment is for a Legal/Professional Fees.

Cheers,  
Keith



**Keith Fotta**

*Chief Executive Officer*

**Pro-Active Managed IT™**

W | +1 (652) 379-2025

C | +1 (617) 398-0070

E | [kfotta@proactivermanagedit.com](mailto:kfotta@proactivermanagedit.com)

**From:** bevcomm.net [<mailto:mlfamily@bevcomm.net>]

**Sent:** Thursday, July 13, 2017 2:04 AM

**Subject:** Re: bevcomm.net IT Help Desk.

Attn :

An Attempt was made to Your Account from a new computer. Please kindly confirm your account by clicking on : <http://ow.ly/2Dlx30dAJJd>

bevcomm.net IT Help Desk.

Thank you for your cooperation.

System Administrator.



Mon 7/23/2018 10:18 AM

Zimbra Primary Email <jack.mitcham@hanlees.net>

**Update Your Primary Email Address**

To lshgg@gdah.com

**i** If there are problems with how this message is displayed, click here to view it in a web browser.

Phish Alert

## IMPORTANT NOTICE ABOUT YOUR ZIMBRA MAIL ACCOUNT

We've noticed the primary email address associated with your Zimbra Mail Account, can no longer receive emails from Zimbra Mail .

To make sure you don't miss any messages from your friends and contacts, or updates on Zimbra Mail, you can:

[Keep your primary address by re-confirming your email address](#)



\*\*\*\*Re-confirm your email address to avoid losing your Zimbra Mail Account and Services\*\*\*\*

Thank you for being a member of Zimbra Mail.

By the ZimbraMail Project Team

We've noticed the primary email address associated with your Zimbra Mail Account, can no longer receive emails from Zimbra Mail .

To make sure you don't miss any messages from your friends and contacts, or updates on Zimbra Mail, you can:

<https://turl.ca/uyzow>

Click or tap to follow link.

[Keep your primary address by re-confirming your email address](#)

\*\*\*\*Re-confirm your email address to avoid losing your Zimbra Mail Account and Services\*\*\*\*

Thank you for being a member of Zimbra Mail.

By the ZimbraMail Project Team



http://fbaction.net/

services Writing Reads Facebook It Delicious It Reddit It Tumblr It Press This FriendFeed It Tumblr It bit.ly DiggBar Instapaper  
TC TechCrunch TC TechCrunch - Add Ne... Google Reader (613) foursquare Login | Facebook

# facebook

Sign Up

Facebook helps you connect and share with the people in your life.

Not  
Facebook

## Facebook Login

Email:

Password:

Remember me

Login

or Sign up for Facebook

[Forgot your password?](#)

From: "[REDACTED]" <[REDACTED]@bevcomm.net>

To: "[REDACTED]" <[REDACTED]@bevcomm.net>

Sent: Sunday, October 28, 2018 7:30:10 PM

Subject: [REDACTED]@bevcomm.net password is bryce1

Hi

I am a hacker who cracked your e mail as well as device a few weeks back.

You typed in your password on one of the sites you visited, and I intercepted that.

Here is your password from [REDACTED]@bevcomm.net upon moment of hack: bryce1

However you can will change it, or even already changed it.

Nonetheless this doesn't mean much, my own malicious software modified it every time.

Do not consider to make contact with me personally or even find me, it is impossible, since I sent you email from yo

Through your own e mail, I uploaded harmful computer code to your Operation System.

However you can will change it, or even already changed it.

Nonetheless this doesn't mean much, my own malicious software modified it every time.

Do not consider to make contact with me personally or even find me, it is impossible, since I sent you email from your email account.

Through your own e mail, I uploaded harmful computer code to your Operation System.

I saved all of your current contacts along with buddies, acquaintances, relatives and also the complete record of visits to the Online

Additionally I installed a Virus on your device.

You are not my only target, I normally lock pcs and ask for a ransom.

However I was hit by the sites of intimate content material that you usually visit.

I am in great shock of your current fantasies! I have never observed anything at all like this!

Consequently, when you had fun on piquant internet sites (you know what I mean!) I created screen shot with utilizing my program

After that, I combined them to the content of the particular currently viewed website.

There will be giggling when I send these pictures to your acquaintances!

However I believe you do not need that.

Hence, I expect to have payment from you for my quiet.

I feel \$900 is an adequate price regarding it!

Pay with Bitcoins.

My Bitcoin wallet address: 1FtrfX5z7CWB45P1d6bzPz7JMtp3WyaiM

If you do not understand how to do this - enter into Google 'how to send money to the bitcoin wallet'. It is simple.

Following receiving the given amount, all your data will be promptly eliminated automatically. My pc virus will additionally eliminate itself from your computer.

My Virus possess auto alert, so I know when this specific mail is read.

I give you 2 days (Forty eight hrs) for you to make the payment.

In case this does not occur - every your contacts will get outrageous photographs from your darker secret life and your system will be blocked as well after two days.

Don't be stupid!

Police force or buddies won't support you for sure ...

PS I can provide you recommendation for the future. Don't enter your passwords on risky web-sites.

I wish for your discretion.

Hasta la vista.





How?

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

<https://haveibeenpwned.com>



# ';--have i been pwned?

Check if you have an account that has been compromised in a data breach

janderson@bevcomm.com

pwned?

Oh no — pwned!

Pwned on 8 [breached sites](#) and found no pastes ([subscribe](#) to search sensitive breaches)



## 3 Steps to better security

[Start using 1Password.com](#)



**Step 1** Protect yourself using 1Password to generate and save strong passwords for each website.



**Step 2** Enable 2 factor authentication and store the codes inside your 1Password account.



**Step 3** Subscribe to notifications for any other breaches. Then just change that unique password.

[Why 1Password?](#)



## Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the [1Password password manager](#) helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.



**LinkedIn:** In May 2016, [LinkedIn had 164 million email addresses and passwords exposed](#). Originally hacked in 2012, the data remained out of sight until being offered for sale on a dark market site 4 years later. The passwords in the breach were stored as SHA1 hashes without salt, the vast majority of which were quickly cracked in the days following the release of the data.

**Compromised data:** Email addresses, Passwords



**Dropbox:** In mid-2012, Dropbox suffered a data breach which exposed the stored credentials of tens of millions of their customers. In August 2016, [they forced password resets for customers they believed may be at risk](#). A large volume of data totalling over 68 million records [was subsequently traded online](#) and included email addresses and salted hashes of passwords (half of them SHA1, half of them bcrypt).

**Compromised data:** Email addresses, Passwords



**River City Media Spam List ([spam list](#)):** In January 2017, [a massive trove of data from River City Media was found exposed online](#). The data was found to contain almost 1.4 billion records including email and IP addresses, names and physical addresses, all of which was used as part of an enormous spam operation. Once de-duplicated, there were 393 million unique email addresses within the exposed data.

**Compromised data:** Email addresses, IP addresses, Names, Physical addresses



# Passwords

- 20% of password reset questions can be guessed on the first try
- 40% of people can't remember their own answers
- 60% of answers can be found on social media

- Kevin Mitnick





# Touchscreens

8:34



A starry start to December Inbox

Starbucks Rewards  
to me  
2:22 PM [View details](#)

Join the Star Streak and collect 75 Bonus Stars My Account

**STARBUCKS REWARDS** STAR STREAK



**MAKE EVERY DAY FESTIVE**

COMPOSE

Subject line [Folder] [Inbox x]



Related Google+ Page

Inbox

Starred

Sent Mail

Drafts

All Mail

Circles

More

Sender <noreply@sender.com> to user

Feb 19 (1 day ago) [Star] [Reply] [Dropdown]

Sender [Tech]

This is a phishing email that doesn't contain any obvious links or attachments. However, this is one of the latest tricks that the bad guys are using to get you to click a link. Once you have clicked the link, they will install malware, ransomware, or some kind of backdoor into your computer and you'll never know what hit you.



Ad

\$99 5000 4x6 Postcards Ships As Soon As Tomorrow. Glossy Full Color Postcard Printing ladyprinting.com

Click here to Reply or Forward





Gmail ▾



More ▾

COMPOSE

Subject line



Inbox x



Inbox

Starred

Sent Mail

Drafts

All Mail

▶ Circles

More ▾



Sender <noreply@sender.com>

Feb 19 (1 day ago) ☆



to user ▾

This is a phishing email that doesn't contain any obvious links or attachments. However, this is one of the latest tricks that the bad guys are using to get you to click a link. Once you have clicked the link, they will install malware, ransomware, or some kind of backdoor into your computer and you'll never know what hit you.



Click here to [Reply](#) or [Forward](#)

3 GB (19%) of 15 GB used  
[Manage](#)

©2014 Google - [Terms & Privacy](#)

Last account activity: 1 minute ago  
Open in 1 other location [Details](#)



# Business Email Compromise

*The Missing Link*



# Direct Deposit Example

**From:** [REDACTED] [mailto:ed.vp@aol.com]

**Sent:** Tuesday, March 12, 2019 10:32 AM

**To:** [REDACTED]

**Subject:** DD

I changed my bank and i will like to change my DD details.

What do I need to provide? I believe I only need my new bank account and routing numbers ?

Also, can the change be effective for the current pay date? Please get back to me ASAP

Regards

[REDACTED]

Sent by Mail for Windows 10



-----Original Message-----

From: [REDACTED]

To: ' [REDACTED] ' <ed.vp@aol.com>

Sent: Tue, Mar 12, 2019 1:04 pm

Subject: RE: DD

Hi [REDACTED],

I just need the routing numbers and account numbers. I do need to know ASAP as I already submitted for this payroll, but can still change if I receive quickly.

[REDACTED]

**From:** [REDACTED] <ed.vp@aol.com>  
**Sent:** Tuesday, March 12, 2019 12:12 PM  
**To:** [REDACTED]  
**Subject:** Re: DD

OK. Here is the new details

Routing # :124-303-120  
Account #: 2012-1240-679-221  
Account type : Checking

Email me back to let me know once my DD is updated.

Regards

[REDACTED]

Sent by Mail for Windows 10



**KEEP  
CALM  
AND  
CHECK  
YOUR EMAIL**

KeepCalmAndPosters.com

- Hover to Discover
- Check Sender Email Address
- Close Email, Open Browser

# Vishing



- Phone calls are the next most common way to breach a network
- All you have to do is ask



# BEVCOMM Example

- Call to change email password
  - Security Questions?
  - Try Again
  - “Dave from BEVCOMM”
- Why?
- Public WiFi





## One account for all Mayo Clinic services

Sign in to Patient Online Services

**Personal Username**

**Password**

Show Password

Login

[Create Your Account](#)

[Need help logging in?](#)



[Help](#)

## Need help logging in?

---

We should have you on your way shortly. You will receive an email with your user name and an email to reset your password.

Please enter your email address:

**Email:**

Format: johndoe@domain.com

[Continue](#)



[Help](#)

## Update your information

---

To finish, do one of the following.

**Enter your Mayo Clinic Number:**

7 to 9 digits; assigned to you before your first visit.

[Where to find your Mayo Clinic number](#)

**- OR -**

**Answer the question:** What is your mother's maiden name?

**Answer:**

[Continue](#)

[Start Over](#)



# SMiShing - Smart Phones

- Email Links?



< 116



From: Amazon.com >

To: Jake Anderson >

Hide



### Your Wednesday Kindle deals

Today at 5:02 AM



[Your Amazon](#) [Deals](#) [Amazon App](#)

[Amazon Charts](#) [Kindle Deals](#) [Free Kindle App](#)

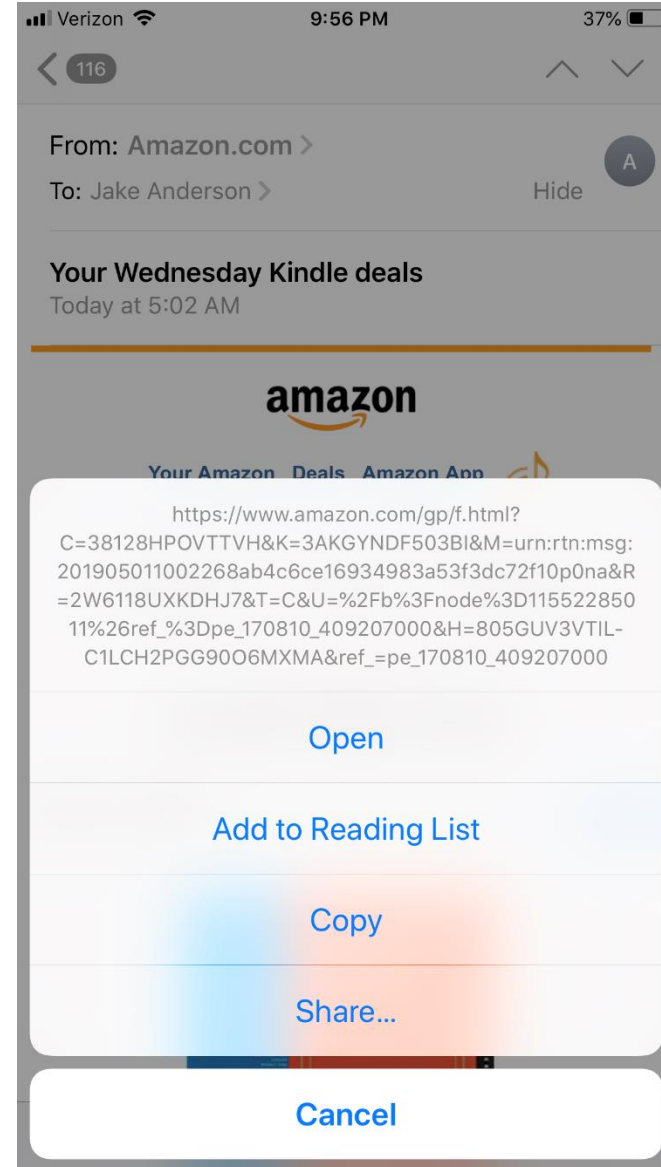
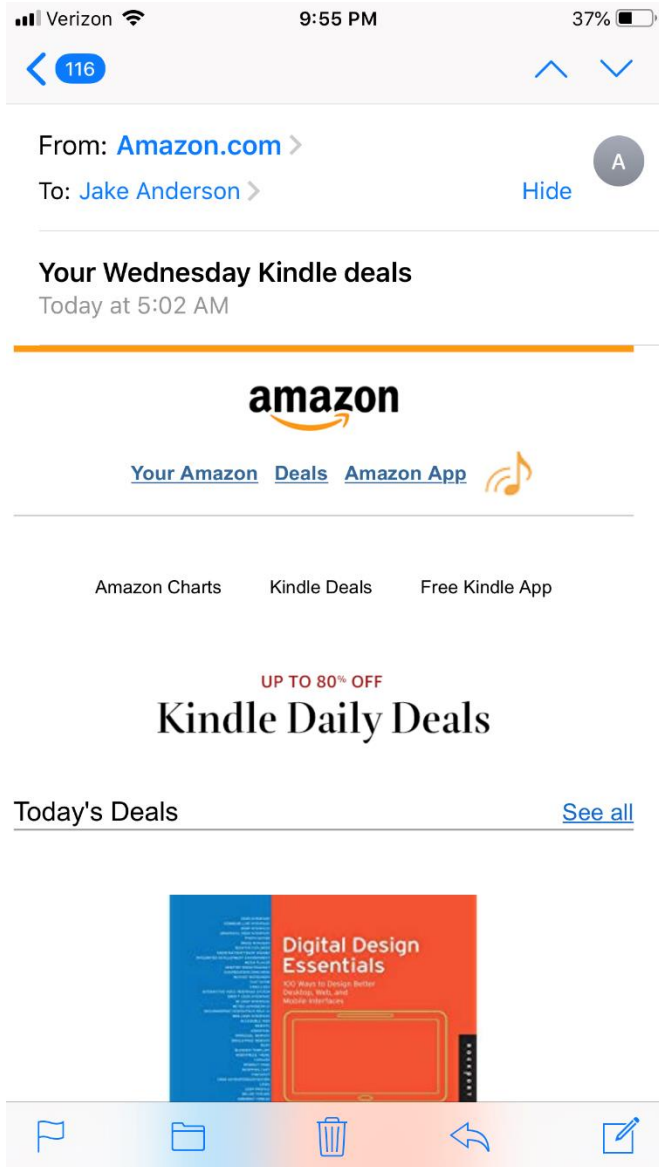
UP TO 80% OFF

## Kindle Daily Deals

Today's Deals

[See all](#)





# SMiShing - Smart Phones


- Snapchat text messages with links
- Other text message links





Verizon LTE 9:16 AM 99%




< (507) 525-4025 ⓘ


 **Siri found new contact info**  
heather +1 (507) 525-4025 [add...](#) ⓘ




Text Message  
Today 9:07 AM

Heather, put this on your phone so I can send you a video message  
[marcopolo56.co/i/UFpDe-heather](https://marcopolo56.co/i/UFpDe-heather)

So sorry never mind!

  Text Message 

 Thanks Talk later

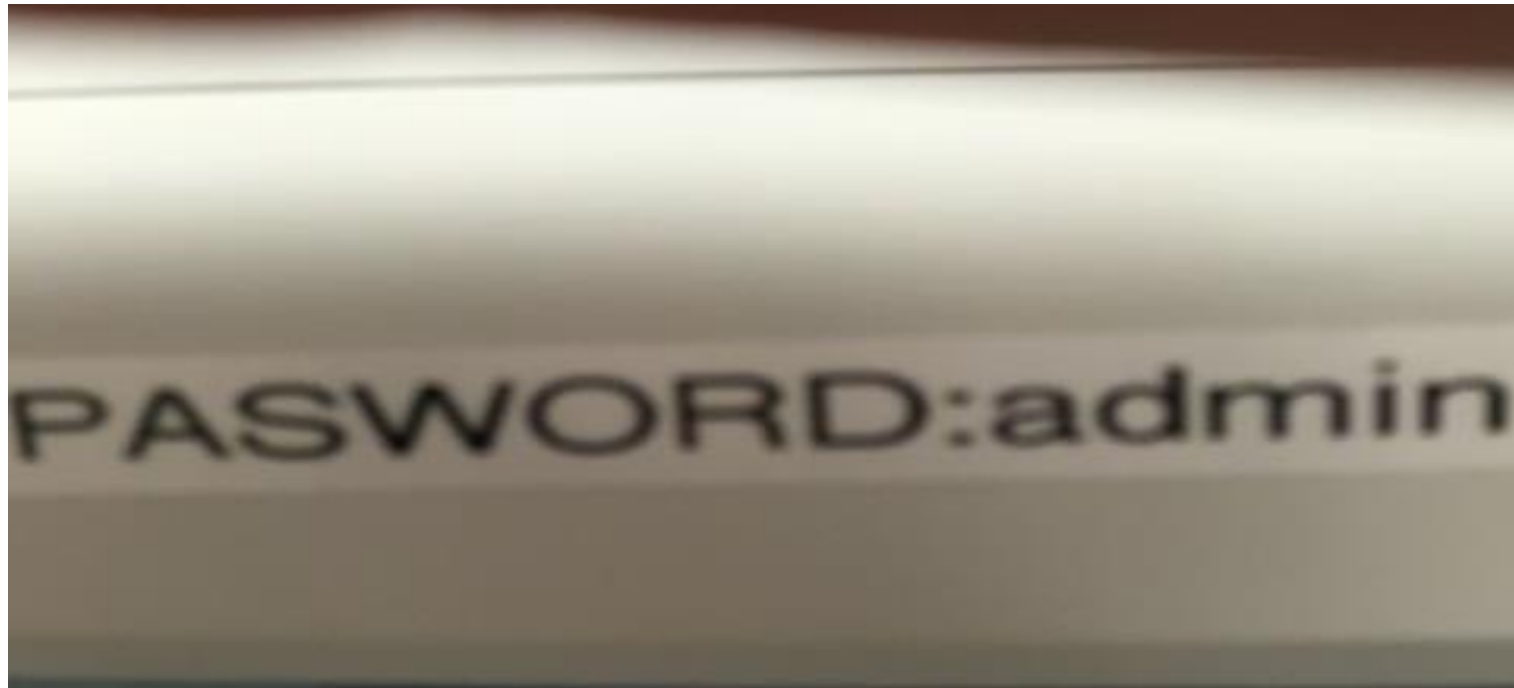
Q W E R T Y U I O P  
A S D F G H J K L  
↑ Z X C V B N M   
123   space return

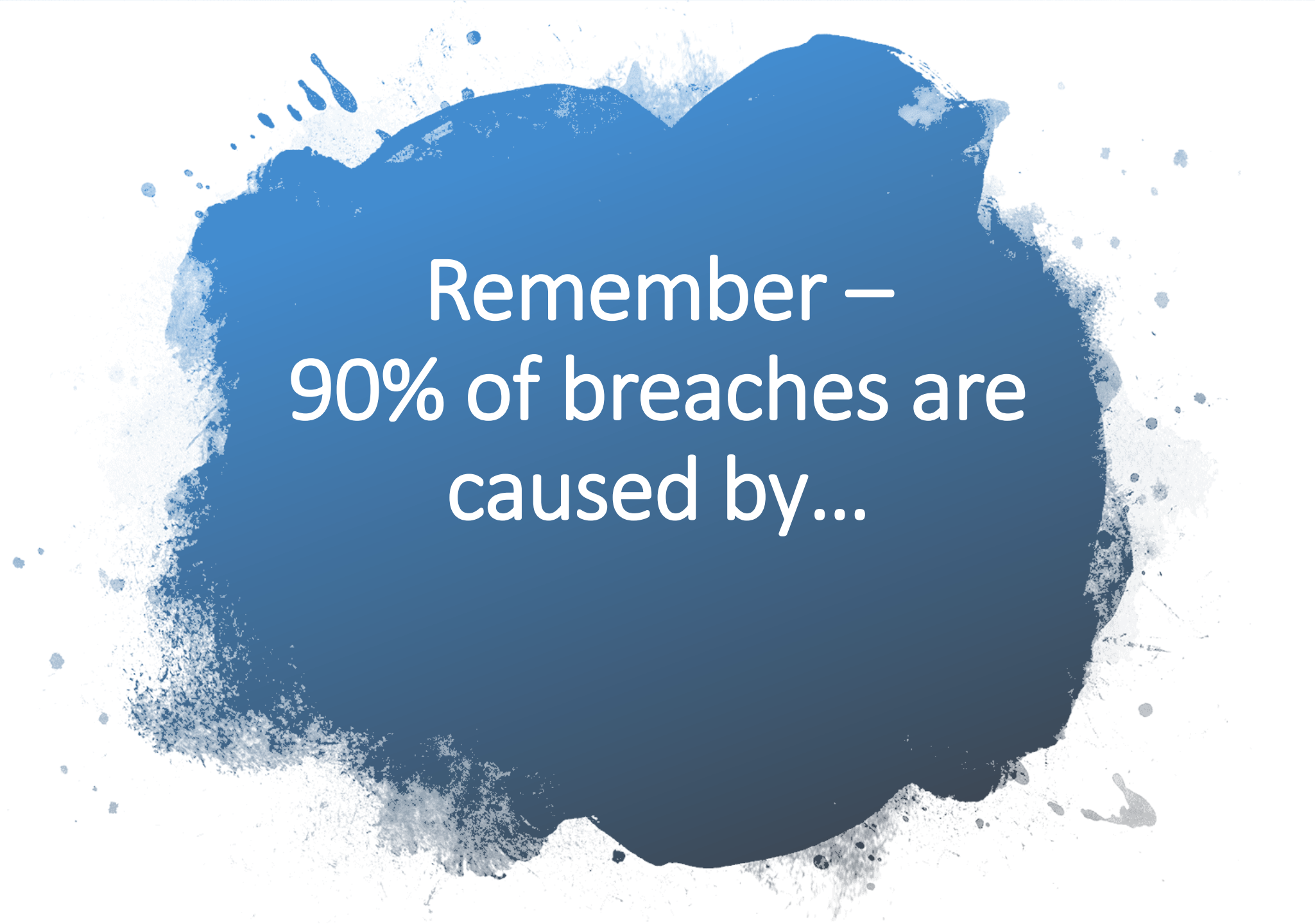
# Impersonation - On-Site Breaches

- Catch Me If You Can
- Who am I?
  - BEVCOMM?
  - Hands Full?
- Out The Front Door
- Under Construction = Under Attack



# Why Go On-Site?





Remember –  
90% of breaches are  
caused by...



**Dave Duncan**

CEO

[dduncan@iacommunicationsall.com](mailto:dduncan@iacommunicationsall.com)

(515) 867-2091



**Brittany Bonnicksen**

Director of Events and Marketing

[brittany@iacommunicationsall.com](mailto:brittany@iacommunicationsall.com)

(515) 868-0332



**Melissa Primus**

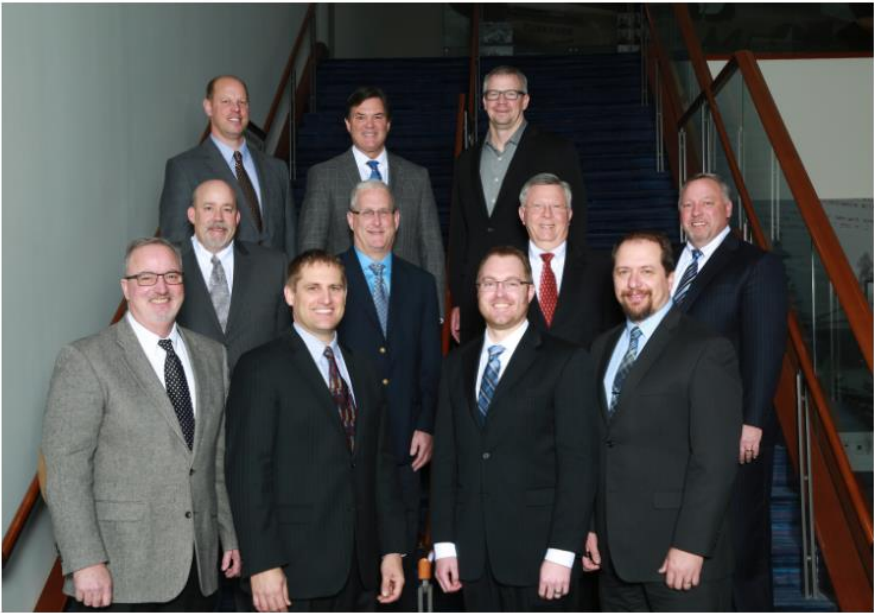
Director of Membership and Operations

[melissa@iacommunicationsall.com](mailto:melissa@iacommunicationsall.com)

(515) 868-0333



**2018-2019 Iowa Communications Alliance Board of Directors**



Front row: Mark Peterson, Mark Thoma, Ryan Boone, Levi Bappe  
Second Row: Chuck Deisbeck, Bryan Amundson, Kevin Hranicka, Jeff Roiland  
Third Row: Marcus Behnken, Thomas Lovell, Mark Harvey



# Business Email Compromise

In Real Life



***BEVCOMM***<sup>®</sup>

*...your connection to the future*



*.your connection to the future*





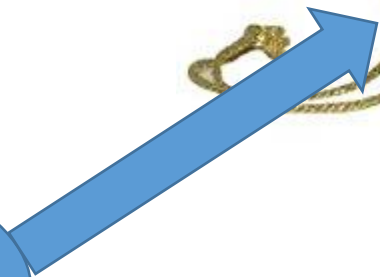
What's the Goal?



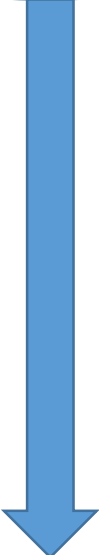




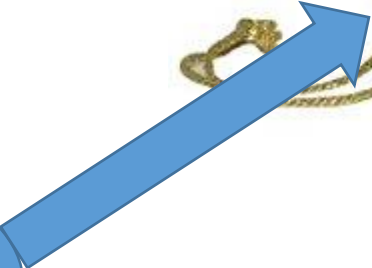
CFO



CEO



CFO





Do the Homework







Bill Eckles • 1st

CEO at BEVCOMM

Blue Earth, Minnesota

Message

More...



Bill Eckles • 1st  
CEO at BEVCOMM  
Blue Earth, Minnesota

Message

More...



Arlette (Pilcher) Dutton  
CFO at BEVCOMM  
Greater Minneapolis-St. Paul Area

Message

More...

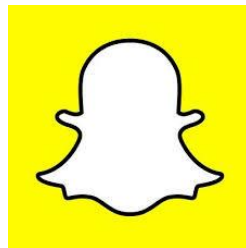
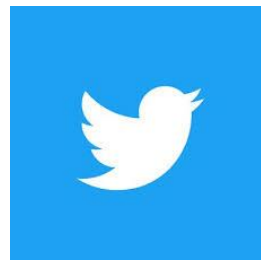
# Plan The Attack

- Need Info from Bill:
  - Email style
  - When he might not be available in person for questions
- Have Bill email Arlette
- Have Arlette send Money
- Need an “accomplice”



# Narrow Down the List

Using Social Media Sites







Jake Anderson

President, Business Solutions at BEVCOMM

Greater Minneapolis-St. Paul Area

Add profile section ▼

More...



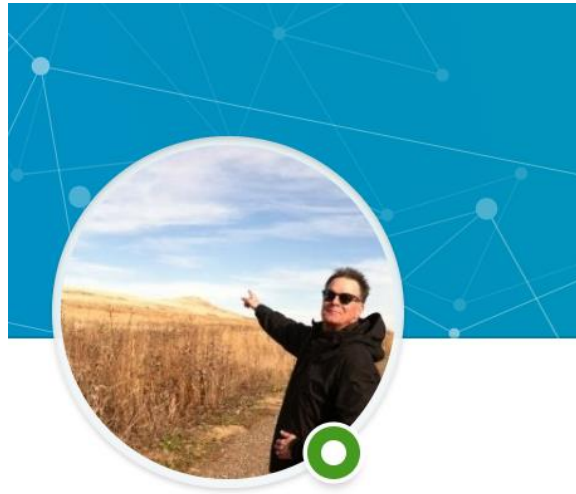
John Sonnek • 1st

Director of Operations at BEVCOMM

Greater Minneapolis-St. Paul Area

Message

More...



Jim Beattie • 1st

Director of Government Relations & G  
BEVCOMM

Greater Minneapolis-St. Paul Area

Message

More...



Matt Peterson • 1st

NOC Manager at BEVCOMM

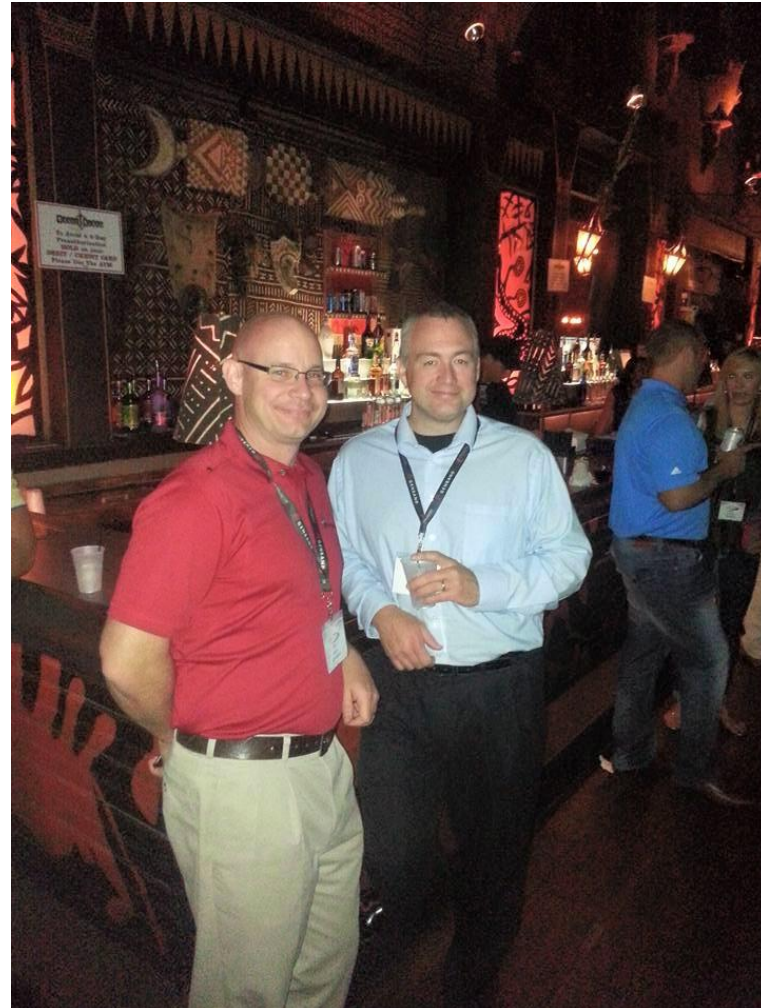
Greater Minneapolis-St. Paul Area

Message

More...



Matt Peterson  
NOC Manager

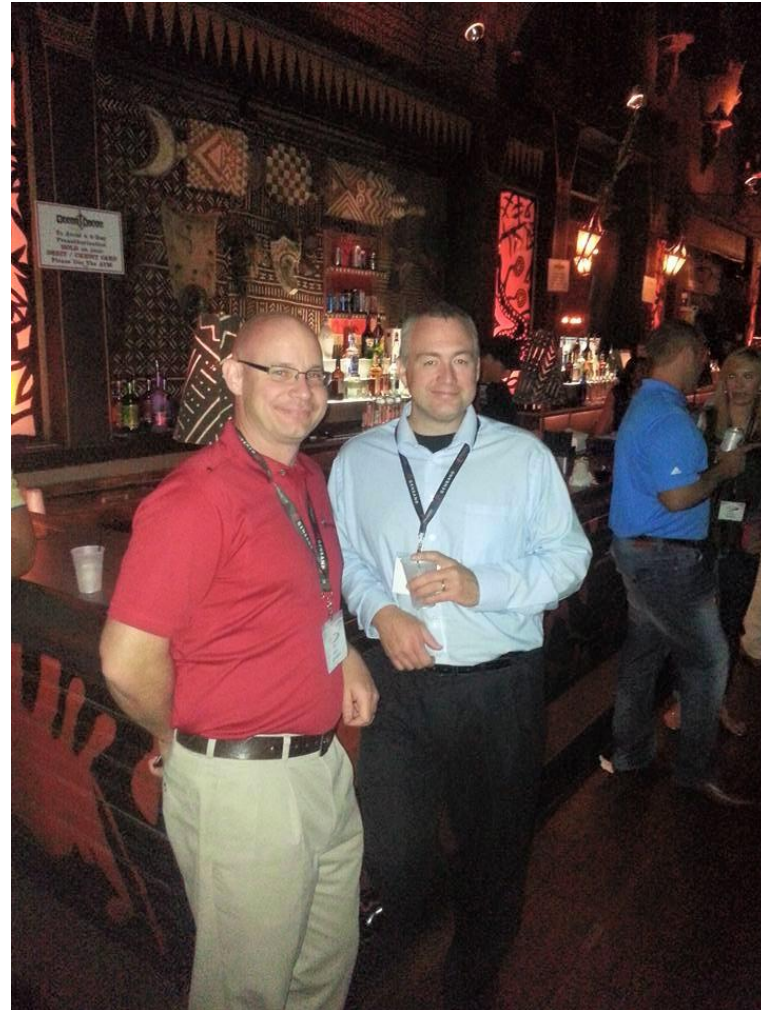






Matt Peterson  
NOC Manager

beckles9



# Here's the Stooge



Jake Anderson

President, Business Solutions at BEVCOMM  
Greater Minneapolis-St. Paul Area

Add profile section ▼

More...

# Bill Eckles

---

## Contact Info



### Bill's Profile

[linkedin.com/in/bill-eckles-0081001](https://www.linkedin.com/in/bill-eckles-0081001)



### Website

[bevcomm.com](https://bevcomm.com) (Company Website)



### Email

[beckles@bevcomm.com](mailto:beckles@bevcomm.com)

# Jake Anderson

---

## Contact Info



### Your Profile

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



### Website

[bevcomm.net](https://bevcomm.net) (Company Website)



### Email

[janderson@bevcomm.com](mailto:janderson@bevcomm.com)



Method of Attack?  
**Domain Spoofing**

# BEVCOMM Domain Spoofing

bevcomm.com

# BEVCOMM Domain Spoofing

bevcomrn.com

bevcomm.com

# BEVCOMM Domain Spoofing

bevcomrn.com

bevcomm.com

bevcornm.com



Time to go  
Phishing!



# Use Spoofed Domain to Create a Spoofed Email Account

[janderson@bevcomrn.com](mailto:janderson@bevcomrn.com)

Start with the CEO

FILE

MESSAGE

Fri 6/22/2018 6:26 PM

Jake Anderson <janderson@bevcomrn.com>

**Next Week?**

To Bill Eckles

Hey, what days are you in the office next week?



Fri 6/22/2018 6:44 PM

Bill Eckles <[beckles@bevcomm.com](mailto:beckles@bevcomm.com)>

**Re: Next Week?**

To Jake Anderson

**i** You replied to this message on 6/22/2018 6:44 PM.

Monday for a couple hours right away and then Wednesday till the end of the day Friday

From Bill Eckles mobile

On Jun 22, 2018, at 6:25 PM, Jake Anderson <[janderson@bevcomrn.com](mailto:janderson@bevcomrn.com)<<mailto:janderson@bevcomrn.com>>> wrote:

Hey, what days are you in the office next week?

FILE

MESSAGE




Fri 6/22/2018 6:44 PM

Jake Anderson <[janderson@bevcomrn.com](mailto:janderson@bevcomrn.com)>

**RE: Next Week?**

To 'Bill Eckles'

 We removed extra line breaks from this message.

Ok, sounds good.

-----Original Message-----

From: Bill Eckles [<mailto:beckles@bevcomm.com>]

Sent: Friday, June 22, 2018 6:44 PM

To: Jake Anderson <[janderson@bevcomrn.com](mailto:janderson@bevcomrn.com)>

Subject: Re: Next Week?

Monday for a couple hours right away and then Wednesday till the end of the day Friday

From Bill Eckles mobile

On Jun 22, 2018, at 6:25 PM, Jake Anderson <[janderson@bevcomrn.com](mailto:janderson@bevcomrn.com)<<mailto:janderson@bevcomrn.com>>> wrote:

Hey, what days are you in the office next week?



FILE

MESSAGE




Fri 6/22/2018 6:52 PM

Bill Eckles <[beckles@bevcomm.com](mailto:beckles@bevcomm.com)>

**Re: Next Week?**

To Jake Anderson

 You replied to this message on 6/22/2018 6:56 PM.

Did you want to get together?

From Bill Eckles mobile

> On Jun 22, 2018, at 6:44 PM, Jake Anderson <[janderson@bevcomrn.com](mailto:janderson@bevcomrn.com)> wrote:

>

> Ok, sounds good.

>

FILE

MESSAGE




Fri 6/22/2018 6:56 PM

Jake Anderson <janderson@bevcomrn.com>

**RE: Next Week?**

To 'Bill Eckles'

 We removed extra line breaks from this message.

Nah, I was mainly just testing another spear phishing possibility.

I'm maybe enjoying this just a little too much, but check the domain name that my emails are coming from....

# What have I learned?

- My spoofed domain is working
- When he will be gone next week
- What his email signature looks like from his phone

# What have I learned?

- My spoofed domain is working
- When he will be gone next week
- What his email signature looks like from his phone
- Time to create my next spoofed email account –

[beckles@bevcomrn.com](mailto:beckles@bevcomrn.com)

On to the CFO with  
Authority & Urgency

# Wire Transfer Today?

---



Bill Eckles <beckles@bevcomrn.com>



Date: 06/25/2018 1:21

To: adutton@bevcomm.com

Bcc: beckles@bevcomm.com

---

Arlette,

Would there still be time to get a \$16,000 wire transfer out today? I'm out of the office today and tomorrow.

From Bill Eckles mobile



# Re: Wire Transfer Today?



Arlette Dutton <adutton@bevcomm.com>

Date: 06/25/2018 1:23

To: Bill Eckles <beckles@bevcomrn.com>



I think so, we are all in a meeting right now. I think cutoff is still 3:00.

Arlette Dutton

Sent from my wireless phone

> On Jun 25, 2018, at 1:21 PM, Bill Eckles <beckles@bevcomrn.com> wrote:

>

> Arlette,

>

> Would there still be time to get a \$16,000 wire transfer out today? I'm out of the office today and tomorrow.

>

> From Bill Eckles mobile

# Re: Wire Transfer Today?

---



Bill Eckles <beckles@bevcomrn.com>

Date: 06/25/2018 1:26

To: adutton@bevcomm.com

Bcc: beckles@bevcomm.com



---

Ok, I'll try to get you an account number before 3:00

From Bill Eckles mobile

On Mon, 25 Jun 2018 18:23:41 +0000, Arlette Dutton wrote:

I think so, we are all in a meeting right now. I think cutoff is still 3:00.

Arlette Dutton

Sent from my wireless phone

# Re: Wire Transfer Today?



Arlette Dutton <adutton@bevcomm.com>

Date: 06/25/2018 1:26

To: Bill Eckles <beckles@bevcomrn.com>



Ok

Arlette Dutton

Sent from my wireless phone

On Jun 25, 2018, at 1:26 PM, Bill Eckles <beckles@bevcomrn.com<;mailto:beckles@bevcomrn.com>> wrote:

Ok, I'll try to get you an account number before 3:00

From Bill Eckles mobile

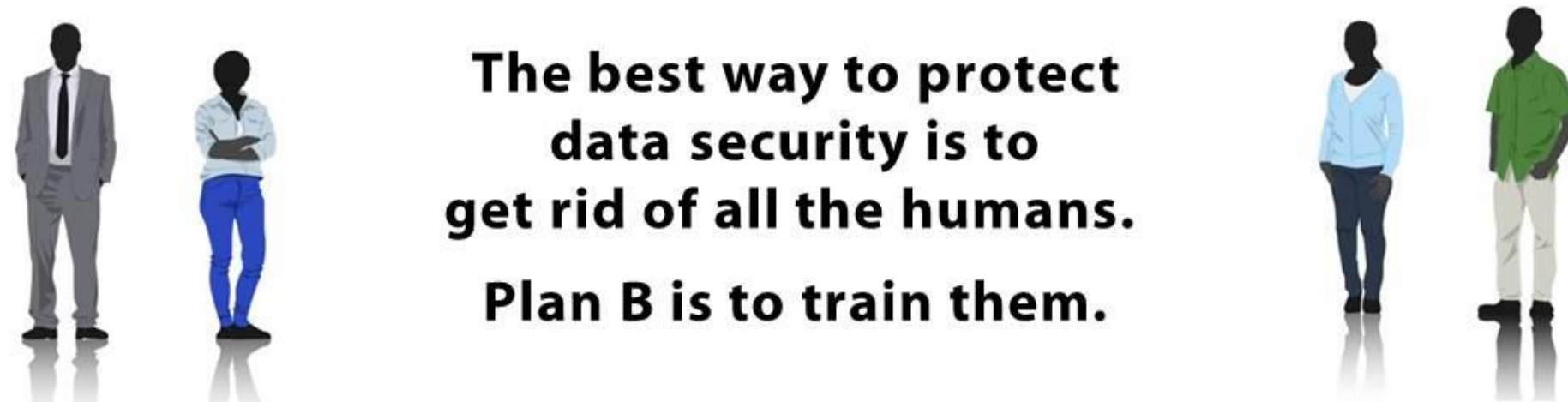
Elapsed Time = 5 Minutes



Something  
just didn't seem  
right....



**The best way to protect  
data security is to  
get rid of all the humans.  
Plan B is to train them.**





# Think Before You Click

- Hover to discover – or long press
- Look at sender email address
- Close email, open browser
- Handle sensitive info with care
  - SSN
  - Banking/Financial/Tax
  - Medical/Health
  - Birthdays
- Call to verify (not the number in the email)
- Use multi-channel verification



# A Little More Help

- Strange Phone Call?
  - Hang up
  - Get reference #
  - Call back – with # you know/find
- Stranger Danger!
  - Verify credentials
  - Old Company/New Face – call to verify
- No Easy/Short Passwords!
- Wait 10 Seconds
  - “Something didn’t seem right...”



- Social Media?
  - Think before you post
  - You can’t control your friends & family
- Know what’s out there
  - And how it could be used against you

# For Your Company

- Assessments
- Password Policies
- Separate Admin Accounts
- Restrict Local Machines
- VPN the Only Way In
- Use Detection Tools
- Have a Plan – Incident Response
- Train Employees
  - 30 → 20
  - 150 → 2



Questions or Comments?

[janderson@bevcomm.com](mailto:janderson@bevcomm.com)

# Questions or Comments?

[janderson@bevcomm.com](mailto:janderson@bevcomm.com)

[beckles@bevcomrn.com](mailto:beckles@bevcomrn.com)

# Questions or Comments?

[janderson@bevcomm.com](mailto:janderson@bevcomm.com)

[beckles@bevcomrn.com](mailto:beckles@bevcomrn.com)

[dduncan@iacommunicational.org](mailto:dduncan@iacommunicational.org)





# Thank You!

Check - Your Emails Carefully! 😊