

Here Phishy Phishy

Kris Morton

CIO BSK Associates

October 18, 2022

BSK Associates

- Engineering, Analytical, and Materials testing firm covering the West Coast
- Approximately 200 employees
- Seven Locations



About Me



- I've worked for BSK since 2016
 - CIO for 4 years
- 15 years of experience in various roles IT and software development
- MBA in IT Management
- Security has been a primary focus since starting with BSK
 - Implemented many of the solutions we are going to discuss today.
- I'm a husband and father of two and I have two 13-month-old granddaughters (born 9 days apart)

Three Fundamental Truths

Bad actors are going to act badly.

Good people click on bad things

No security system is infallible

Some Fun Numbers

- Phishing incidents increased by 110%, from 114,702 incidents in 2019 to 241,324 incidents in 2020. (FBI, 2020)
- Business Email Compromise attacks caused losses of 1.8 billion in 2020. (FBI, 2020)
- One of the main vectors of ransomware is malicious phishing emails. (Verizon, 2020)
- 91% of cyber attacks come from email. (Phishme, 2017)

[2020 IC3Report](#)

[2021 Data Breach Investigations Report | Verizon](#)

[PhishMe-Phishing-Defense-Guide_2017.pdf \(ciosummits.com\)](#)

The Human Firewall

Harden Employees



Security Awareness Training



Test your employees regularly.



Train the entire person not just about work

Don't Take the Bait (Awareness Training)

Phishers rely on your trust.

Questions you should ask?

- Is there a sense of urgency created?
- Is this a typical communication ?
- Who sent it

Just because it comes from your domain does not mean it is real (spoofing)

Never open an attachment you weren't expecting

- Go old school. Call the person to confirm authenticity

A blue ribbon graphic with a 3D effect, featuring a darker blue shadow on the left side. The ribbon is horizontal and contains the text "Testing the Users" in white.



Testing the Users

Account Refund Verification Status - Message (HTML) Search

File Message Help Mimecast PDF-XChange


Share to Teams Mark Unread Find Zoom Reply with Meeting Poll

Account Refund Verification Status

 Amazonom <amazonom@order-refunds.com>
To  Kris Morton

Reply Reply All Forward

Tue 10/4/2022 3:16 PM

 Your Account | Amazon

Message From Customer Service

Hello,

Has your email or mobile number changed?

We cannot process your last order due to a mismatch on your card/billing address. Please confirm your account (www.account-activity.com/amazom-youraccount) now to avoid interruptions.

We appreciate your business and look forward to serving you again in the near future.

Best regards,
Mary M.

Amazonom

From: Amazon <amazom@order-refunds.com>

Template ID:498629-2434492

Reply-To: Amazon <amazom@order-refunds.com>

Subject: Account Refund Verification Status

 Send Me a Test Email

Show Remote Images

 Toggle Red Flags




Your Account | Amazon



Message From Customer Service

Hello,

Has your email or mobile number changed?

We cannot process your last order due to a mismatch on your card/billing address. Please confirm your account (www.account-activity.com/amazom-youraccount) now  to avoid interruptions.

We appreciate your business and look forward to serving you again in the near future.

Best regards,
Mary M.

Amazon



Close

I need help updating my bank account info - Message (HTML) Search

File Message Help Mimecast PDF-XChange

Share to Teams Mark Unread Find Zoom Reply with Meeting Poll

I need help updating my bank account info

 Kimberly Tavarez <kimberly.t@bskassociates.com>
To  Kris Morton

Reply Reply All Forward

Tue 10/4/2022 3:28 PM

Start your reply all with: [Yes, I can do that.](#) [It has been updated.](#) [We will take care of it.](#) [Feedback](#)

Hello,

I was told to contact someone in HR to update my bank account info. Would someone be able to do this before the upcoming pay period?

Here is the document showing my account information that it needs to be updated to:
[Account information.pdf](#)

Thanks so much for your help!

Kimberly Tavarez
Customer Support
Email: Kimberly.T@bskassociates.com



```
https://secured-login.net/  
xdxjzspwh0dhmbzoi8vc2dvjdxjjwzc1svb  
2dpbi5ukzxkqvcgfnzxmvmzc3ymq4snda  
1mwvjimvtywlsx3rlbxbsyxrlx2lkptexnju3  
ndgmywn0aw9upxbyzxzpzxcmdxnlcl9pz  
d01mde1njgyoq==  
Click or tap to follow link.
```

I need help updating my bank account info - Message (HTML) Search

File Message Help Mimecast PDF-XChange

Share to Teams Mark Unread Find Zoom Reply with Meeting Poll

I need help updating my bank account info

 Kimberly Tavaréz <kimberly.t@bskassociates.com>
To  Kris Morton

Reply Reply All Forward

Tue 10/4/2022 3:28 PM

Start your reply all with: [Yes, I can do that.](#) [It has been updated.](#) [We will take care of it.](#) [Feedback](#)

Hello,

I was told to contact someone in HR to update my bank account info. Would someone be able to do this before the upcoming pay period?



Here is the document showing my account information that it needs to be updated to:
[Account information.pdf](#)

Thanks so much for your help!

Kimberly Tavaréz
Customer Support
Email: Kimberly.T@bskassociates.com

```
https://secured-login.net/  
xdxjzspwh0dhmbzoi8vc2dvjdxjjwzc1svb  
2dpbi5ukzxkqvcgfnzxmvmzc3ymq4snda  
1mwvjjmvtywlsx3rlbxbsyxrlx2lkptexnju3  
ndgmywn0aw9upxbyzxzpzxcmdxnlcl9pz  
d01mde1njgyoq==  
Click or tap to follow link.
```

De-activation of kmorton@bskassociates.com in Process

 Microsoft 365 <security@security-microsoft.usa>
To  Kris Morton

Reply Reply All Forward

Tue 10/4/2022 3:27 PM

Microsoft 365 Email Essentials

Hello Kris



Confirm Your Email kmorton@bskassociates.com

Your incoming messages are queued and pending delivery on your account kmorton@bskassociates.com. We require you to confirm your account with a security challenge to protect your account.

[Confirm Account](#)

Thanks,
The Microsoft account team

De-activation of kmorton@bskassociates.com in Process

 Microsoft 365 <security@security-microsoft.usa>
To  Kris Morton

Reply Reply All Forward

Tue 10/4/2022 3:27 PM

Microsoft 365 Email Essentials

Hello Kris

Confirm Your Email kmorton@bskassociates.com

Your incoming messages are queued and pending delivery on your account kmorton@bskassociates.com. We require you to confirm your account with a security challenge to protect your account.

[Confirm Account](#)

Thanks,
The Microsoft account team

File Message Help Mimecast PDF-XChange

admin.bskassoc...
To Manager
Team Email

Delete Archive
Delete Respond
Share to Teams
Move
Tags
Editing
Immersive
Translate
Zoom
Zoom
Reply with Meeting Poll
Viva Insights
Phish Alert Report
Phish Alert

Suspicious Message

This message may be an attempt to obtain sensitive information.

Report Phishing

Mail

You Need to Read This NOW!



Donna Morton <krionna@gmail.com>

To Kris Morton

Reply Reply All Forward

Mon 10/10/2022 1:30 PM



You won't believe what your dog did. It is going to cost us a TON of money.

Best Regards,

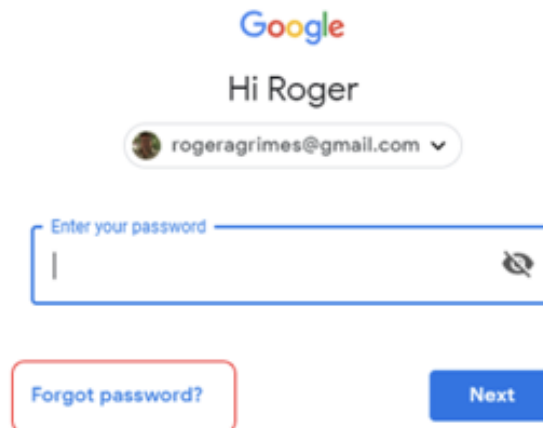
Donna



Other Type of Attacks (Funny Names)

- SMISHING (Sending text messages with links or urgent requests)

From Google Security: We have detected a rogue sign-in to your goodguy@gmail.com account credentials. In order to determine the legitimate login we're going to send a verification code to your previously registered phone number from another Google support number. Please re-type the sent verification code in response to this message or your account will be permanently locked.



Google

Hi Roger

rogeragrimes@gmail.com

Enter your password

Forgot password? Next

Your Google verification code is [954327](#)

From Google Security: We have detected a rogue sign-in to your goodguy@gmail.com account credentials. In order to determine the legitimate login we're going to send a verification code to your previously registered phone number from another Google support number. Please re-type the sent verification code in response to this message or your account will be permanently locked.

[954327](#)

Sent

I Don't Name These Things

- VISHING- Voice Phishing
- Tech Support
 - In 2018, people [reported losing](#) over \$55,000,000 in tech support scams according to the Federal Trade Commission (FTC)
 - Apple and Microsoft.
- Twitter
 - Attackers made vishing calls to Twitter's tech support impersonating Twitter IT Support
 - The attackers' instructions were simple, "we need you to reset your password."
 - It worked
 - Usernames, Passwords and MFA info was used to access the Twitter's back-end
 - Led to the hijacking of high-profile Twitter accounts.

What to do with the Suspicious Email

- Send it to all your co-workers and ask them if they think it is suspicious?
- Don't Reply, Forward, or mark as Spam
- Report it to your IT Department



Train the Entire Person

This isn't just about work!

Work Life Blending (A Security Nightmare)

- The boundaries between work and life have been blurred.
- Many companies are allowing personal devices to access company resources
- Phishing personal emails can lead to compromised work credentials
- Training Programs should include information about cyber criminal's use of social media to extract key data points

Train and Test Your Employees

- Simulate Attacks
- Regular Training
- Test Again
- Gamification
- Automate Software

Three Fundamental Truths

**BAD ACTORS
ARE GOING
TO ACT BADLY.**

**GOOD PEOPLE
CLICK ON BAD
THINGS**

**NO SECURITY
SYSTEM IS
INFALLIBLE**