The Importance of Multi-Factor Authentication on Cyberhealth for Health Care Providers and Facilities

March 24, 2022

KAMMCO

Presenters

Brandon Welch is a California licensed attorney who has been with Beazley for nearly three years as part of the Breach Response Services team. In his role as a Breach Response Manager, he assists insureds through data security incidents on behalf of the insurance company and assists in educating insureds. In his free time, he enjoys going on long runs, learning languages, and spending time with his wife.

Presenters

Shawn Weldin is the Director of Information Technology and HIPAA Security Officer at Sabetha Community Hospital, in Sabetha KS. As the director he oversees all technology within the hospital, rural health clinic and home health and hospice agency operated by SCH. Shawn holds several Microsoft Certifications and has over 20 years experience in both cyber and physical security. He also serves as the President of Kansas HIMSS.

Presenters

Andy Grittman joined KAMMCO in 1996, and since 2006 has served as Vice President and Chief Information Officer. He is the former President of the Board of Directors of the Oasis Customer Group, and former chair of the technology subsection for the Medical Professional Liability Association Technology, Human Resources and Finance (THRF) section. Mr. Grittman graduated from Washburn University and proudly served in the United States Army.

Housekeeping Items

From: Jacqueline Grunau jgrunau@kammco.com

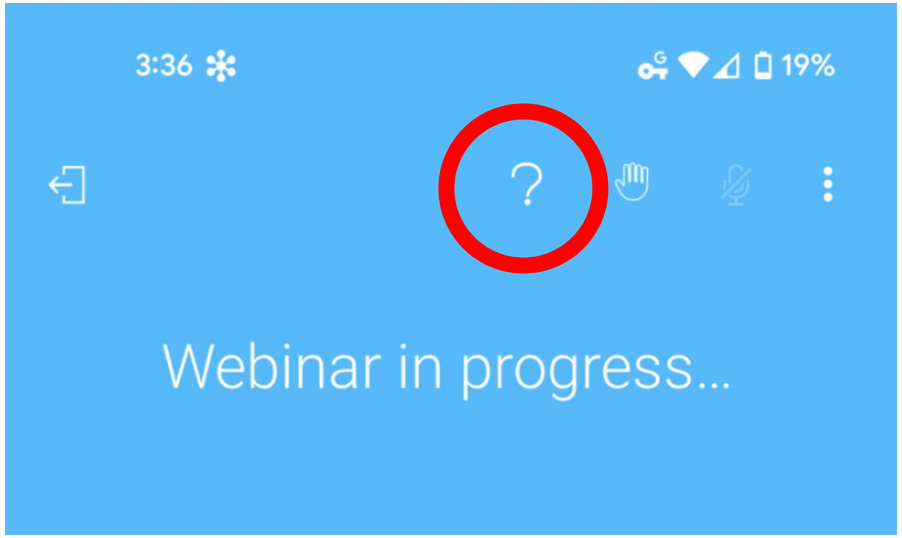
Subject: Slides from today's presentation

Housekeeping Items

Recording available in the **Education Library** on the KAMMCO website: www.kammco.com.

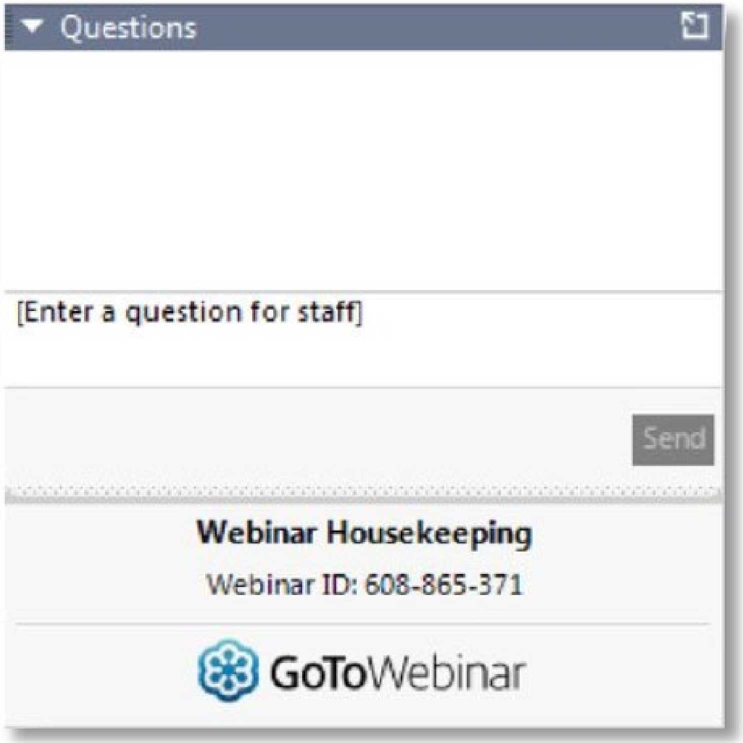
Housekeeping Items

Mobile or Tablet App



Webinar in progress...

Desktop Controler



[Enter a question for staff]

Webinar Housekeeping

Webinar ID: 608-865-371

Housekeeping Items

Your feedback matters!

Housekeeping Items

Two more Spring Education Webinars
www.kammco.com/events

The Importance of Multi-Factor Authentication on Cyberhealth for Health Care Providers and Facilities

KAMMCO

Breach Response Services - Beazley

Breach Response Services Team

- Started in 2009
- Handled over 22,000 incidents since 2009

Incident Response

- Managing initial response from the insurance company
- Educating insureds about hard policy issues and breach response
- Coordination of Breach Response Services

Risk Management

- Internal/External stakeholder education on privacy/security issues

MFA (Multi-Factor Authentication)

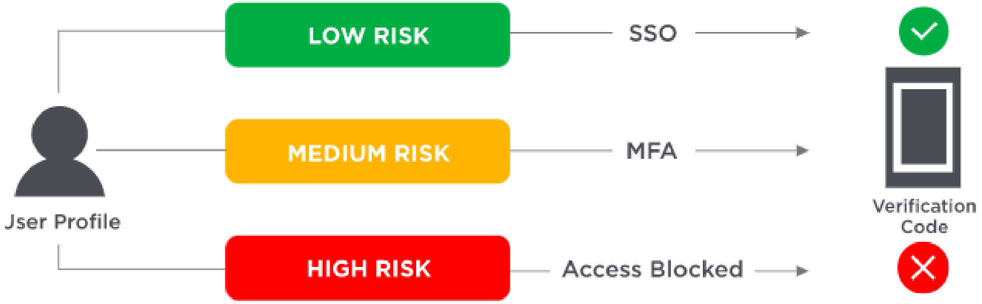
Traditional MFA

- Something you know
  - Password or PIN code
  - Secret answer

- Something you possess
  - Certificate installed on laptop
  - OTP generated by smartphone app (ex. Authenticator)
  - OTP sent via SMS or Email
  - Access badge, USB Device, Smart Card, security key

Recent MFA developments

- Location-based
- Risk-based or Conditional access
  - From where?
  - When?
  - From which device?
  - Which network?
  - Which access?



MFA (Multi-Factor Authentication)

Why not having MFA for external access is very dangerous

- Password leaks and credential stuffing:
  - *Credential stuffing is the automated injection of breached username/password pairs in order to fraudulently gain access to user accounts. This is a subset of the brute force attack category: large numbers of spilled credentials are automatically entered into websites until they are potentially matched to an existing account, which the attacker can then hijack for their own purposes.*
- Password reuse problem (related to human behaviour)
- Hard to detect and defend against
- Very easily automatable with readily available *free* tools
- Credential lists are accessible at very cheap prices (About $5 per database)

Bonus

- https://haveibeenpwned.com/
- https://www.dehashed.com/

REPORTS

Police forces pipe 225 million pwned passwords into 'Have I Been Pwned?'

Posted: December 21, 2021 by Pieter Arntz

Claim Example #1 Ransomware, Mid-Sized Regional Hospital

- Insured is a Mid-sized regional hospital. In the morning, the insured IT system noticed that they were unable to access certain systems. Upon investigating, the IT team realized that they had lost their administrative privileges. Insured began responding immediately in pulling their local back-ups off the network. They subsequently notified Beazley and began utilizing their downtime procedures to ensure continuity of care.

- The Breach Response Services (BRS) team connected their team with a digital forensics service provider and privacy counsel within the hour to begin the investigation and containment. Additionally, the Beazley team walked the insured through all the services available through the policy, despite the insured not thinking PR/Crisis Comms and a Ransomware Negotiator was not necessary.

- The next day, the insured discovered their local back-ups were corrupted or were in a format that may take weeks to recover. Additionally, a local news station has picked up on the story. The insured was able to take necessary and quick business decision to engage the negotiator and PR Crisis Comms team to continue with the remediation and restoration. Insured unfortunately had to pay, but they were able to pivot because of the BRS team.

- It appeared that the bad actor was able to infiltrate the system by compromising a user email account, then elevating their privileges and moving laterally into other systems.

Claim Example #2 Ransomware, Small Practice

- Insured is a solo medical practitioner as an OB/GYN. The insured’s support staff went to log on one morning to discover that they were unable to do so. They immediately called their outsourced IT MSP who attempted to log onto the network but discovered that everything was locked up. The MSP looked to find a ransomware note. Insured tried to work with their MSP to restore their back-ups but found that their last back up was several months before the incident. The insured then notified the insurance carrier of the incident.

- The insurance carrier spoke with the insured to triage the incident. Our team connected the insured with the most economic options for privacy counsel and digital forensics under their policy to ensure that there was additional coverage under their policy, per the insured’s instruction, for other coverages. Using a ransomware negotiator, forensics, and privacy counsel, the insured was able to recover within the week.

- Unfortunately, the insured was compromised to begin with because the MSP account was compromised. There was no MFA on the service account allowing anyone access into the environment once that account was compromised.

Sabetha
MFA Implementation

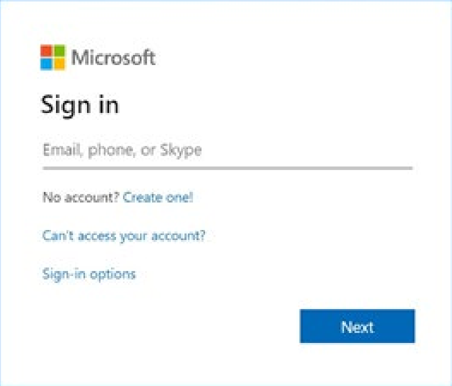
Sabetha Hospital

- 25 Bed Critical Access Hospital
- 160 Employees
- Rural Health Clinic
- Home Health and Hospice
- Outreach Clinic – 45+ Non-Staff Providers

Sabetha Community Hospital • Sabetha Family Practice • NCHH&H •

Microsoft 365

Login



Microsoft

Sign in

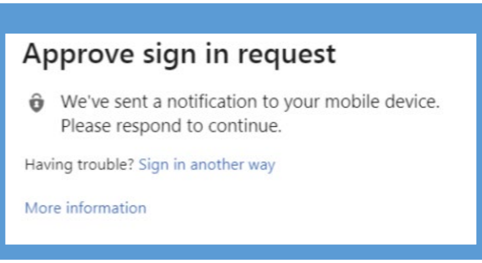
Email, phone, or Skype

No account? Create one!

Can't access your account?

Sign-in options

App

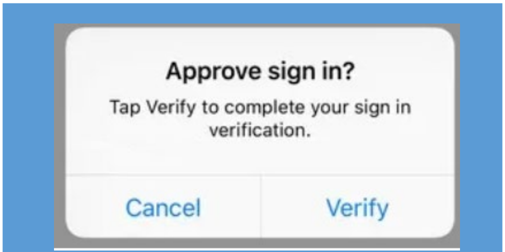


Approve sign in request

We've sent a notification to your mobile device. Please respond to continue.

Having trouble? Sign in another way

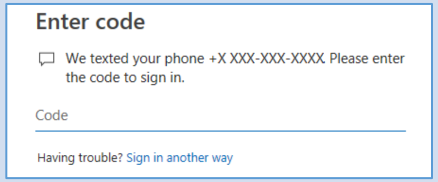
More information



Approve sign in?

Tap Verify to complete your sign in verification.

Text

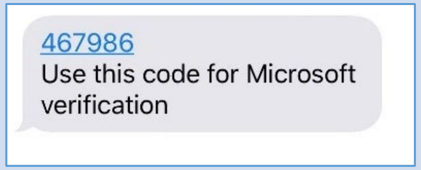


Enter code

We texted your phone +X XXX-XXX-XXXX. Please enter the code to sign in.

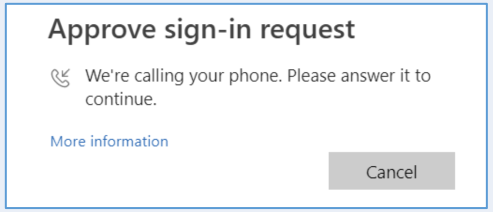
Code

Having trouble? Sign in another way



467986
Use this code for Microsoft verification

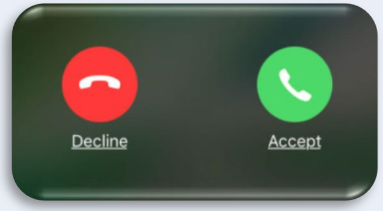
Call



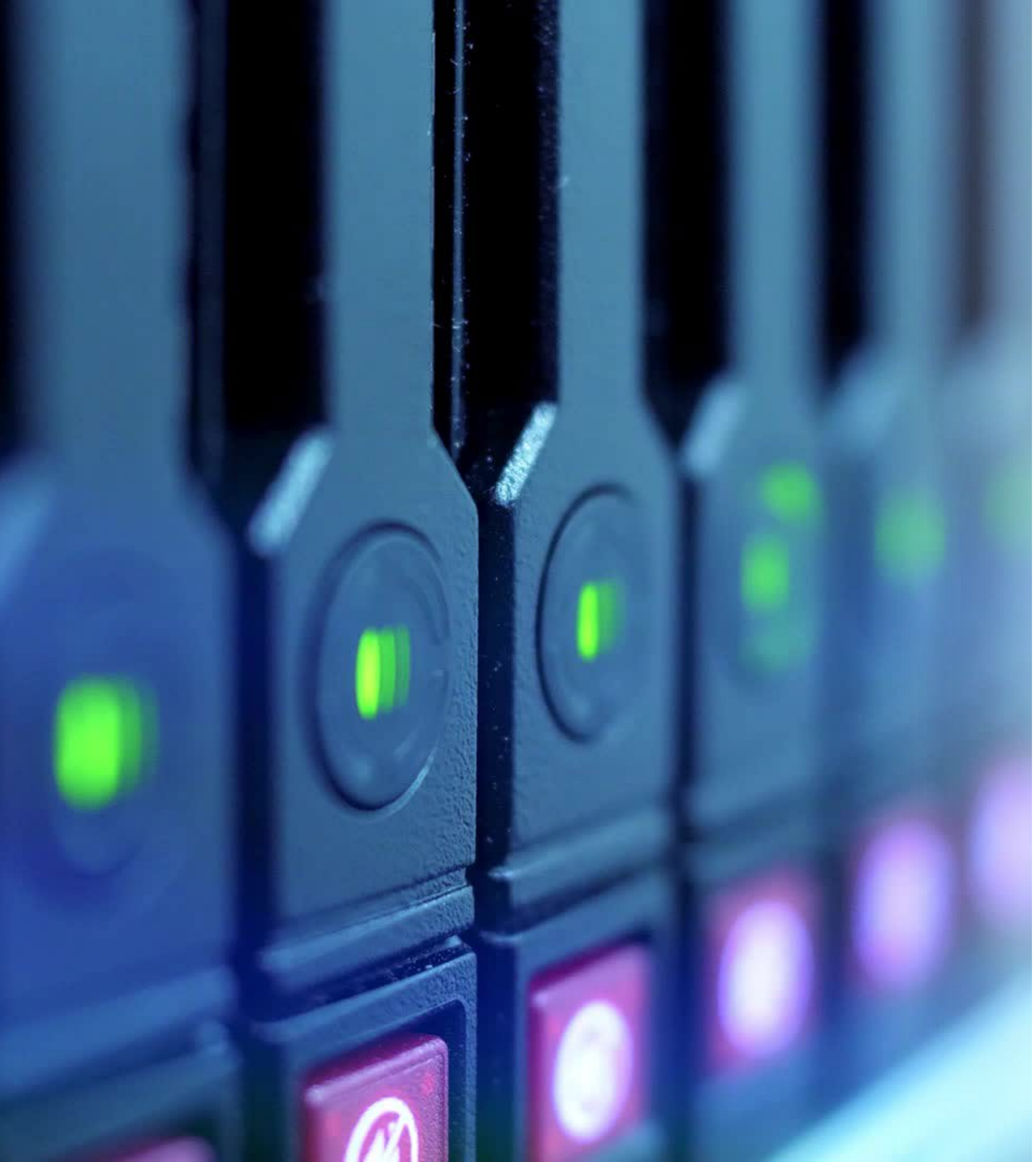
Approve sign-in request

We're calling your phone. Please answer it to continue.

More information



✓



Pre-Enforcement

Setup Conditional Access

- Allows known locations and devices to bypass MFA

Geo Filtering

- Blocking sign-ins from outside the US

Tested with Superusers

Verified that Apps Supported Modern Authentication

- Older versions of Outlook
- Copiers
- Internal software (Helpdesks, Alerting, Notifications)

Day 1

Enabled MFA

- Does not require for login, but allows for the setup

Scheduled Meetings with Departments

- Walked staff through setting up their MFA
  - Started with Department Heads
    - Worked with their staff to setup
  - One-on-one
  - Small group meetings
  - Set schedule for enforcement (Day 3)

Day 3 – Enforced MFA

Troubleshooted any issues

Helped anyone else not setup

- Mostly night shift nursing or PRN staff
- 95% enrollment within 1 week

Items to remember

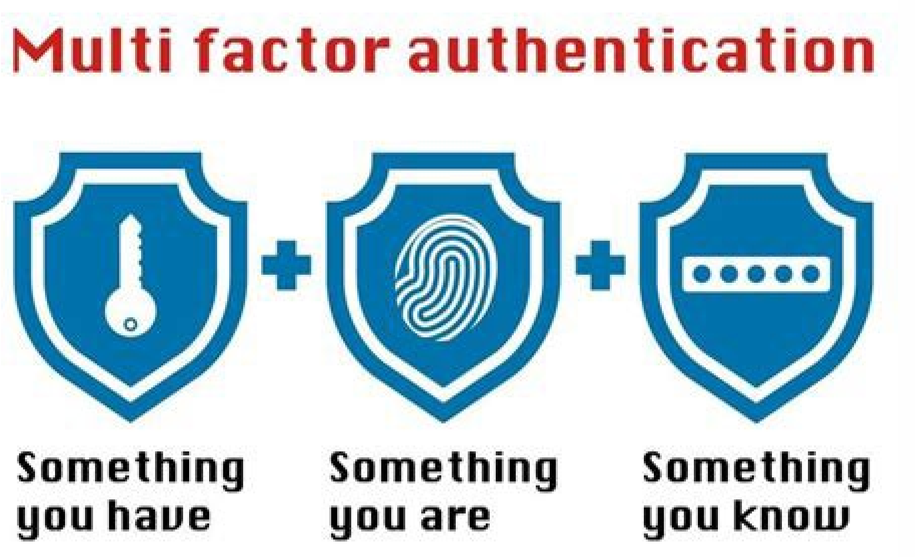
Disable Legacy Authentication

Setup Conditional Access

Coming Next

KAMMCO
MFA Implementation

MFA or 2-FA?


Multi factor authentication
Something you have
Something you are
Something you know

Two Factor Authentication
username
Security PIN
submit
Your Security PIN is:
8496

KAMMCO 2-FA Objectives

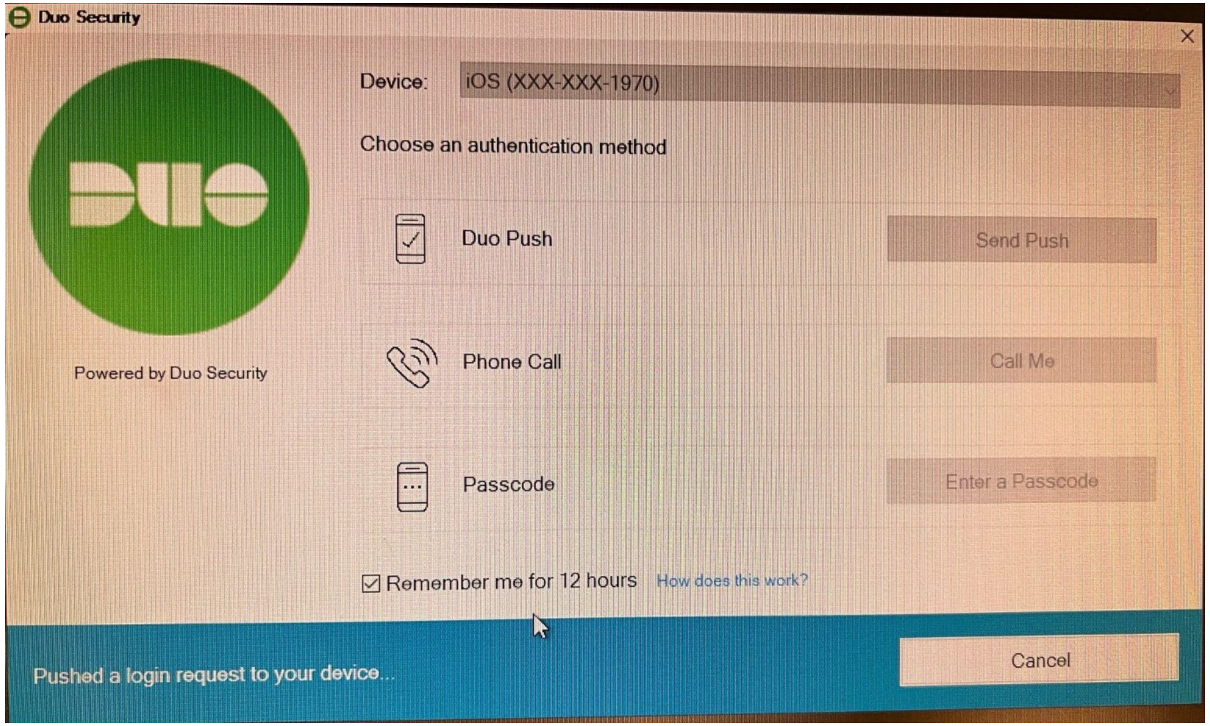
Ease of use

Protect remote access to network, access to cloud environment, and workstation access

Solutions

Proof of Concept

Authentication Options



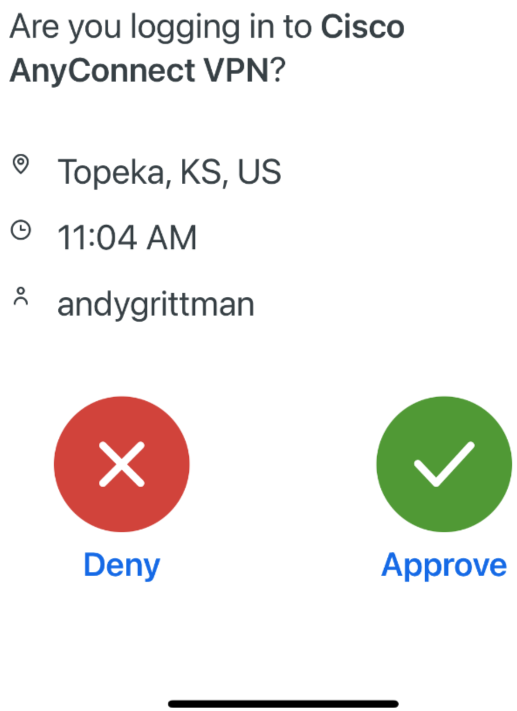
Device: iOS (XXX-XXX-1970)

Choose an authentication method

☑ Remember me for 12 hours

Pushed a login request to your device...

Remote Access (VPN)



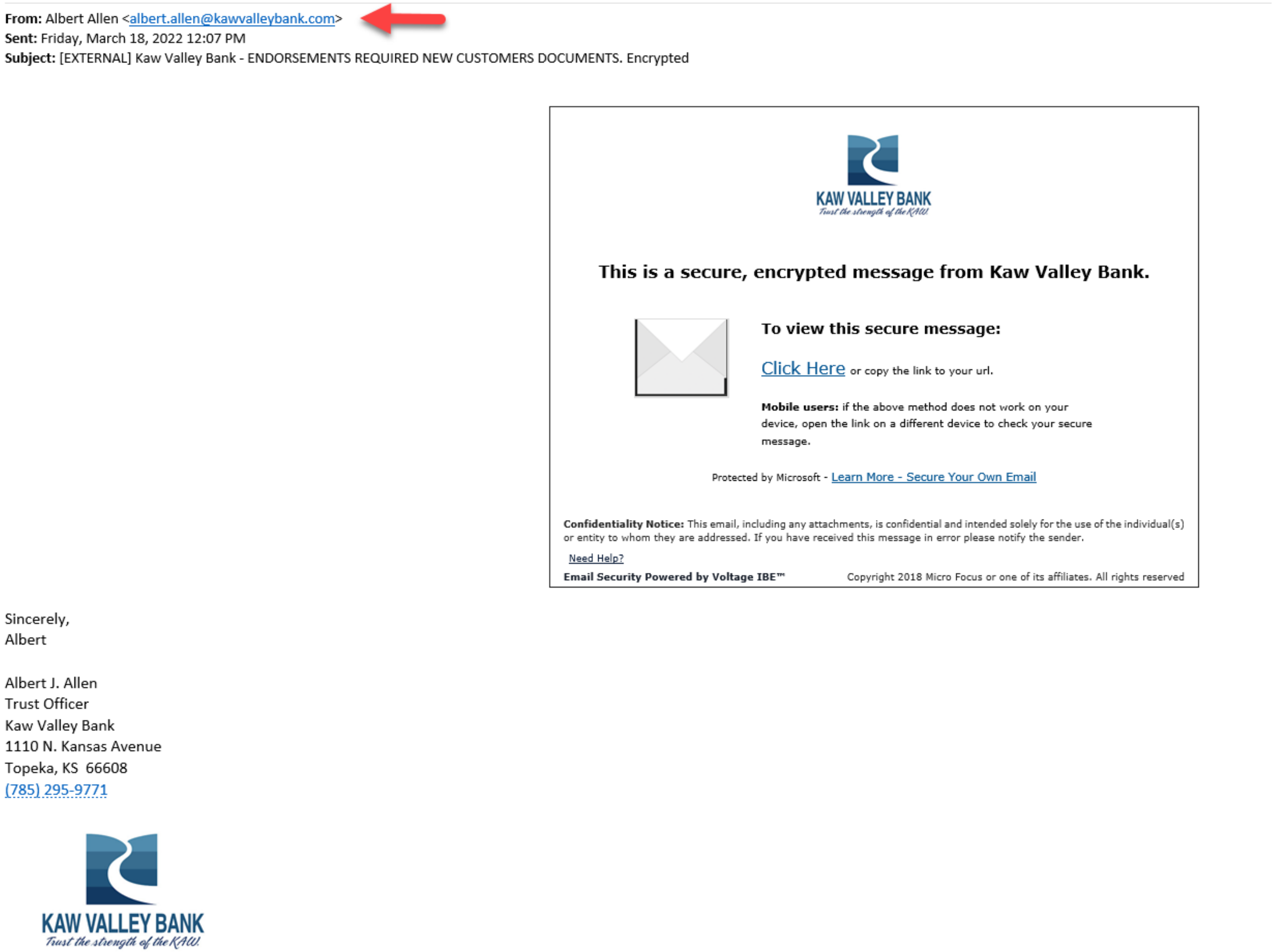
Are you logging in to **Cisco AnyConnect VPN**?

Topeka, KS, US

11:04 AM

andygrittman

Microsoft 365



From: Albert Allen <albert.allen@kawvalleybank.com>
Sent: Friday, March 18, 2022 12:07 PM
Subject: [EXTERNAL] Kaw Valley Bank - ENDORSEMENTS REQUIRED NEW CUSTOMERS DOCUMENTS. Encrypted

KAW VALLEY BANK
Trust the strength of the KAW

This is a secure, encrypted message from Kaw Valley Bank.

To view this secure message:

Click Here or copy the link to your url.

Mobile users: if the above method does not work on your device, open the link on a different device to check your secure message.

Protected by Microsoft - Learn More - Secure Your Own Email

Confidentiality Notice: This email, including any attachments, is confidential and intended solely for the use of the individual(s) or entity to whom they are addressed. If you have received this message in error please notify the sender.

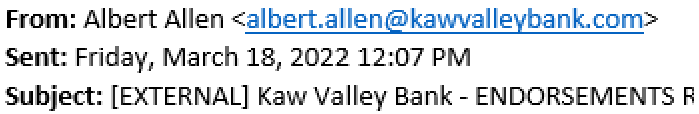
Need Help?

Email Security Powered by Voltage IBE™ Copyright 2018 Micro Focus or one of its affiliates. All rights reserved

Sincerely,
Albert

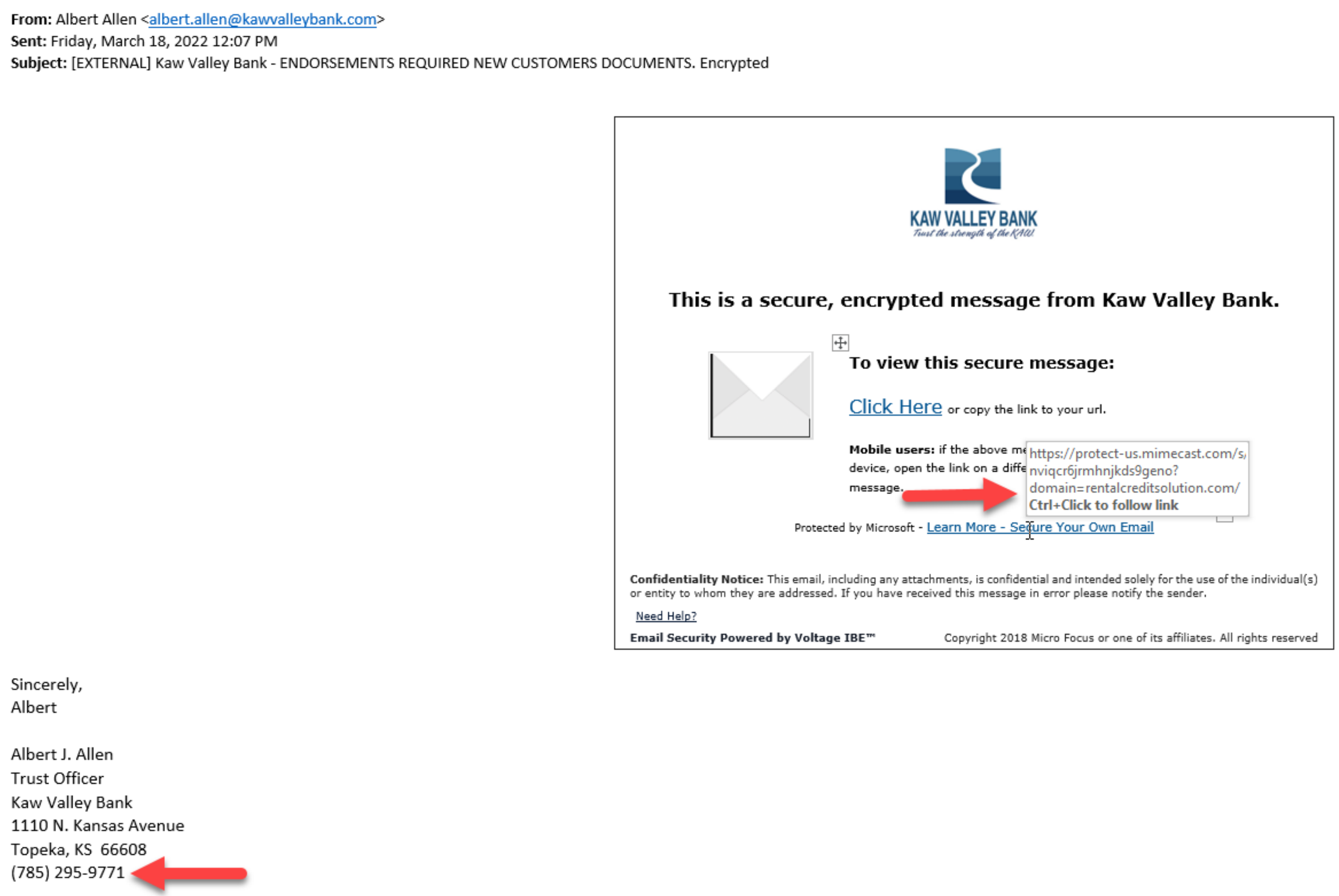
Albert J. Allen
Trust Officer
Kaw Valley Bank
1110 N. Kansas Avenue
Topeka, KS 66608
(785) 295-9771

KAW VALLEY BANK
Trust the strength of the KAW



From: Albert Allen <albert.allen@kawvalleybank.com>
Sent: Friday, March 18, 2022 12:07 PM
Subject: [EXTERNAL] Kaw Valley Bank - ENDORSEMENTS R

Microsoft 365



From: Albert Allen <albert.allen@kawvalleybank.com>
Sent: Friday, March 18, 2022 12:07 PM
Subject: [EXTERNAL] Kaw Valley Bank - ENDORSEMENTS REQUIRED NEW CUSTOMERS DOCUMENTS. Encrypted

KAW VALLEY BANK
Trust the strength of the KAW

This is a secure, encrypted message from Kaw Valley Bank.

To view this secure message:

Click Here or copy the link to your url.

Mobile users: if the above me
device, open the link on a diffe
message.

https://protect-us.mimecast.com/s/
nviqcr6jrmhnjkds9geno?
domain=rentalcreditsolution.com/
Ctrl+Click to follow link

Protected by Microsoft - Learn More - Secure Your Own Email

Confidentiality Notice: This email, including any attachments, is confidential and intended solely for the use of the individual(s) or entity to whom they are addressed. If you have received this message in error please notify the sender.

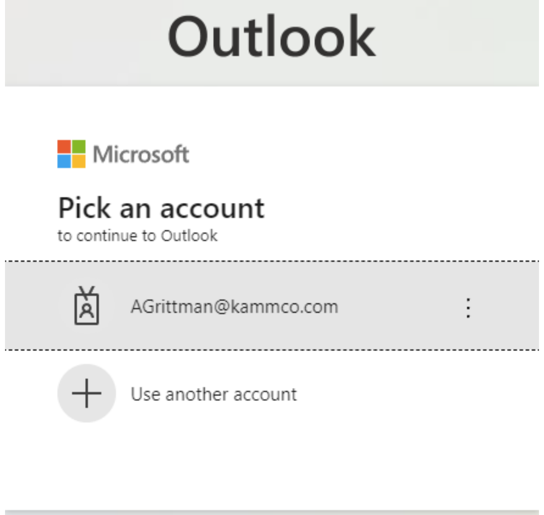
Need Help?

Email Security Powered by Voltage IBE™ Copyright 2018 Micro Focus or one of its affiliates. All rights reserved

Sincerely,
Albert

Albert J. Allen
Trust Officer
Kaw Valley Bank
1110 N. Kansas Avenue
Topeka, KS 66608
(785) 295-9771

Microsoft 365



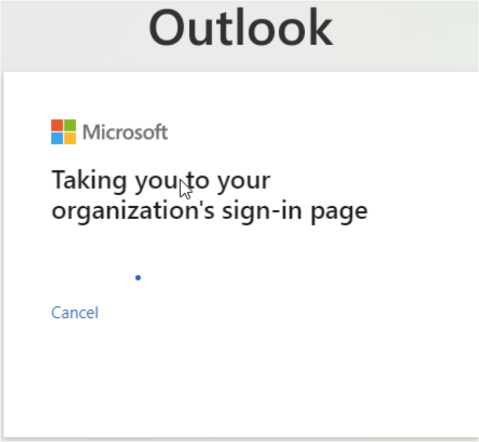
Outlook

Microsoft

Pick an account

to continue to Outlook

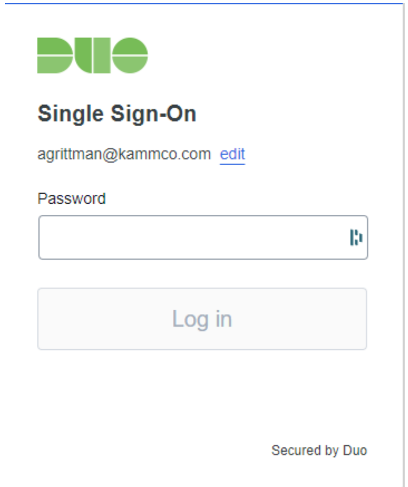
AGrittman@kammco.com



Outlook

Microsoft

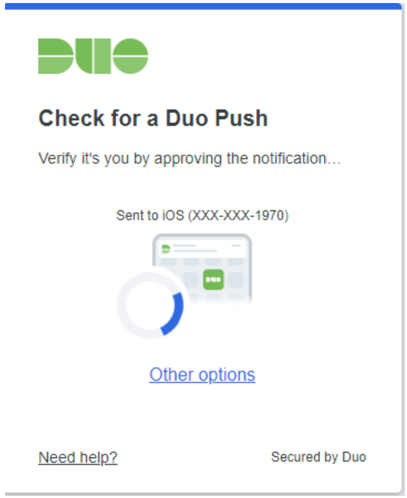
Taking you to your organization's sign-in page



Single Sign-On

agrittman@kammco.com edit

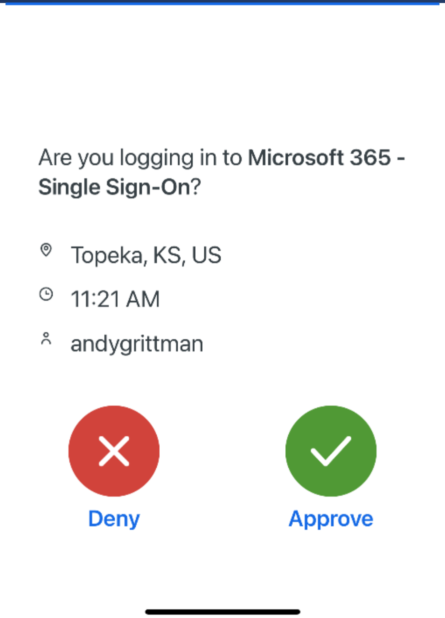
Password



Check for a Duo Push

Verify it's you by approving the notification...

Sent to iOS (XXX-XXX-1970)



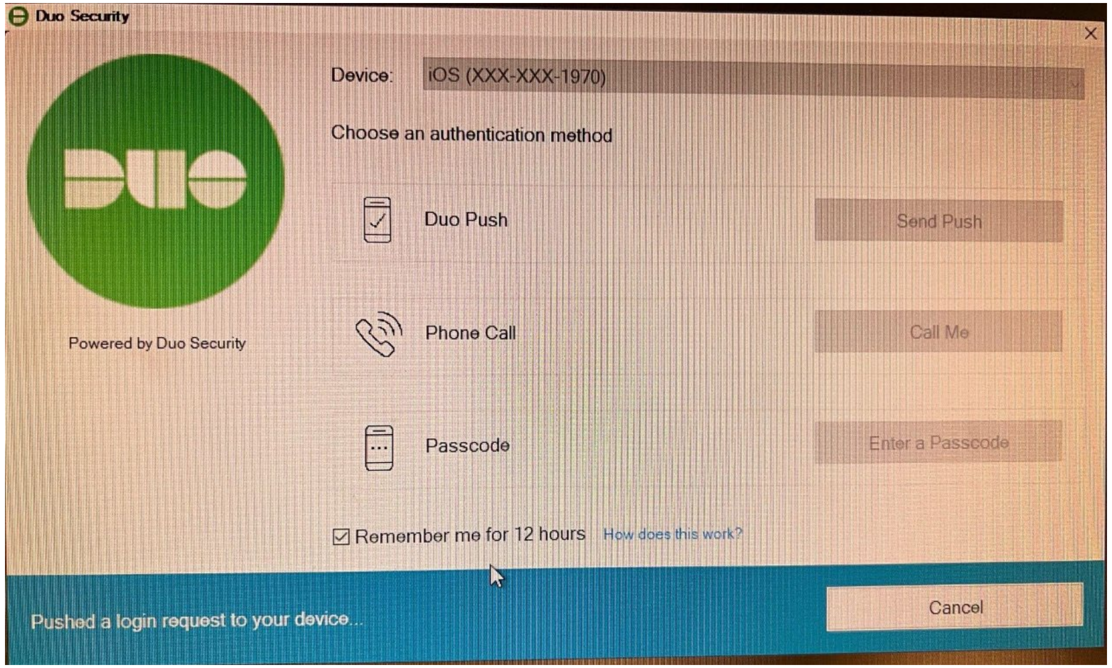
Are you logging in to **Microsoft 365 - Single Sign-On**?

Topeka, KS, US

11:21 AM

andygrittman

Windows Workstation



Device: iOS (XXX-XXX-1970)

Choose an authentication method

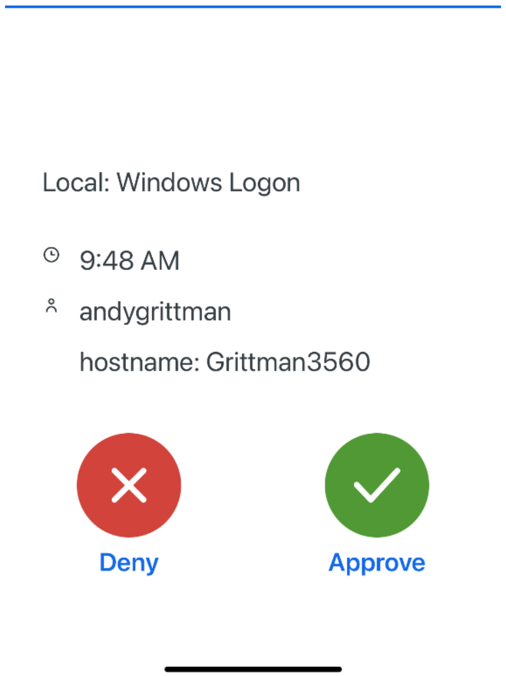
Duo Push

Phone Call

Passcode

☑ Remember me for 12 hours How does this work?

Pushed a login request to your device...



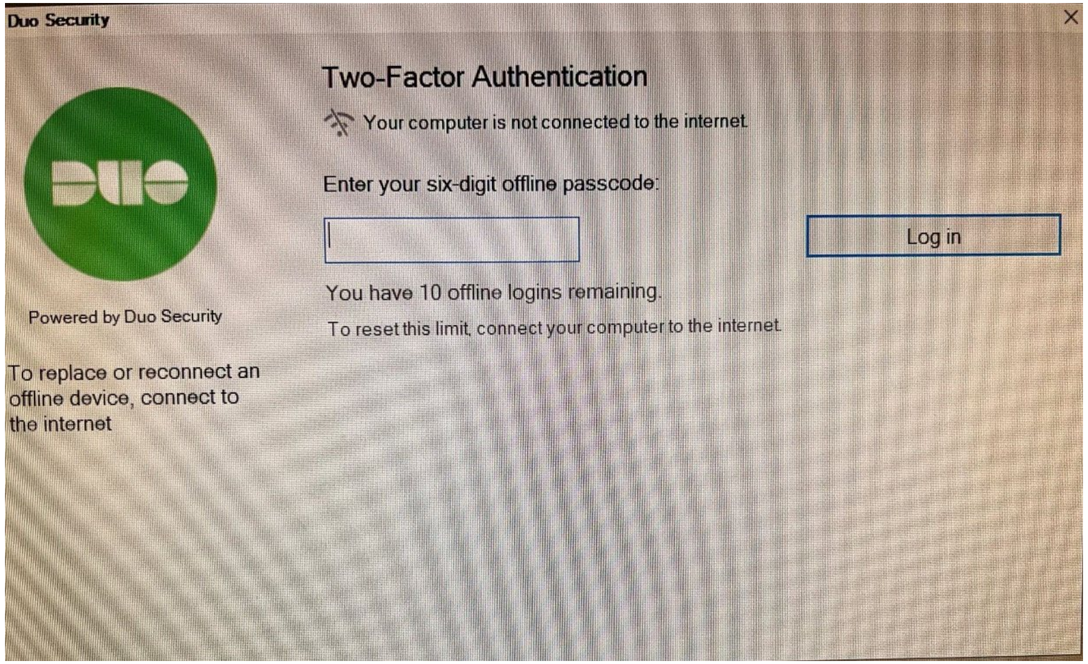
Local: Windows Logon

9:48 AM

andygrittman

hostname: Grittman3560

Windows Offline Authentication



Duo Security

Two-Factor Authentication

Your computer is not connected to the internet.

Enter your six-digit offline passcode:

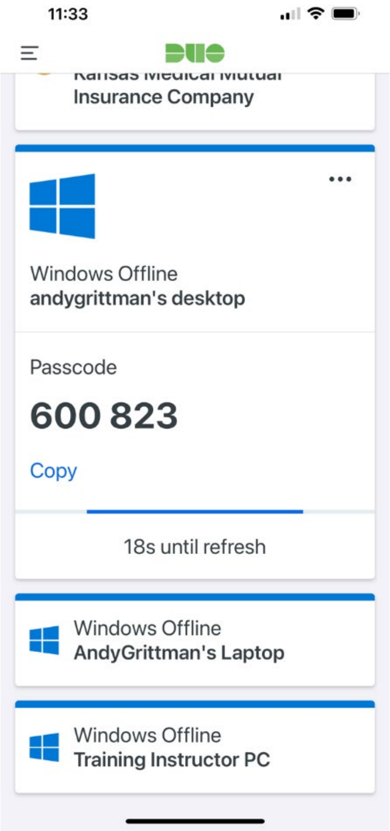
Log in

You have 10 offline logins remaining.

To reset this limit, connect your computer to the internet.

Powered by Duo Security

To replace or reconnect an offline device, connect to the internet



11:33

Kansas Medical Mutual Insurance Company

Windows Offline
andygrittman's desktop

Passcode

600 823

Copy

18s until refresh

Windows Offline
AndyGrittman's Laptop

Windows Offline
Training Instructor PC

Deployment

Next Steps…

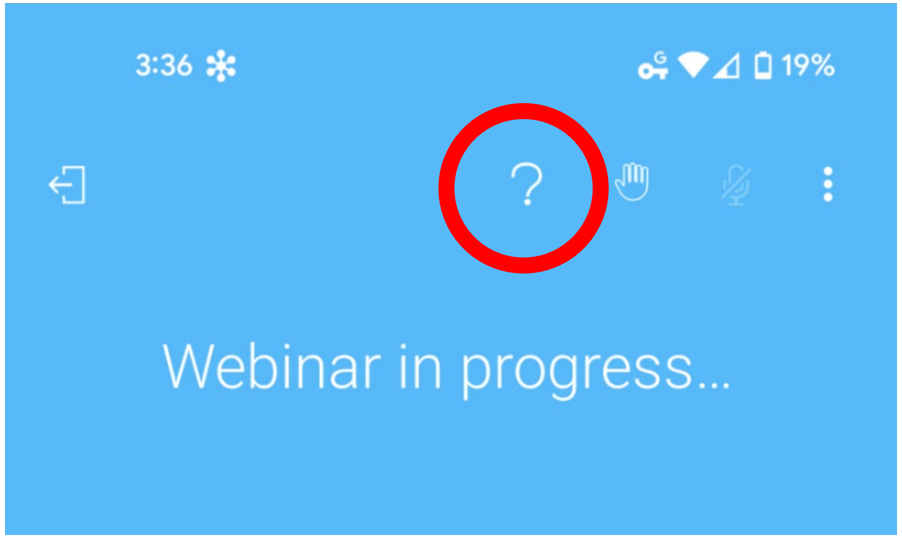
Questions

KAMMCO

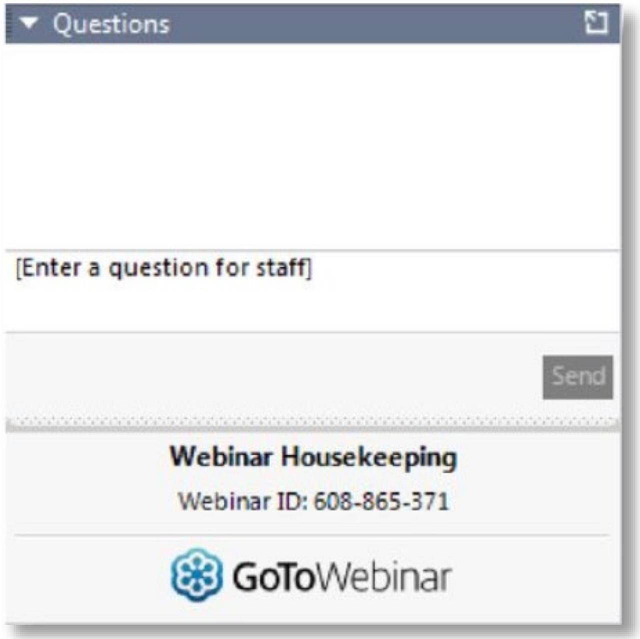
Question & Answer

Submit your questions for our presenters in the GoTo App or Desktop Controller.

Mobile or Tablet App



Desktop Controller



Webinar Housekeeping

Webinar ID: 608-865-371

Question & Answer

Submit your questions for our presenters in the GoTo App or Desktop Controller.

Email additional questions to Jacqueline Grunau at jgrunau@kammco.com.

You can always call us at **1-800-232-2259**.

Thank You!

We appreciate you joining us today.

You'll receive today's slides and a PDF of MFA resources.

Your feedback is appreciated!

Recording available in the **Education Library** on the KAMMCO website: www.kammco.com.

www.kammco.com/events

KAMMCO