GOD DAMN MFA!

CrucialLogics

consulting with a conscience™

Question while we wait!

☑ What are you hoping to get out of this webinar?

Thank you for joining us today!

- This session is being recorded for replay
- Listen-only mode during the presentation
- Ask questions! Please submit questions via the chat

About CrucialLogics

CrucialLogics is Canada’s Leading Microsoft Security Solutions Partner.

We specialize in securing your organization using Native Microsoft Technologies!

2022 Microsoft Canada Impact award winner as a breakthrough partner of the year

#ConsultingWithAConscience

Microsoft

Microsoft Canada Impact Awards

2022 WINNER

Microsoft
Solutions Partner
Security

Specialist
Threat Protection

Microsoft
Cloud Solution Provider

Microsoft
Partner
Microsoft

Gold Collaboration and Content
Gold Cloud Productivity
Gold Cloud Platform
Gold Data Analytics
Gold Datacenter
Silver Small and Midmarket Cloud Solutions
Silver Appiication Development
Silver Windows and Devices
Silver ISV

IT COMPANIES
50
BEST
MANAGED

Speaker

Amol Joshi

Partner Enterprise Services, CrucialLogics

Amol is a senior security executive with over 18 years of experience in leading and executing complex IT transformations and security programs. He’s a firm believer in achieving security through standardization, avoiding complexity and that security be achieved using native, easy-to-use technologies. Amol approaches business challenges in a detail-oriented way and demonstrates quantifiable results throughout the course of highly technical and complex engagements.

Today's Agenda

- ☑ Authentication Factor
- ☑ MFA by-pass via social engineering
- ☑ MFA by-pass via MFA Fatigue
- ☑ Common Issues with MFA Deployments
- ☑ Tips to prevent MFA compromises
- ☑ MFA by-pass via session hijacking
- ☑ MFA by-pass via SIM hijacking

What are the 3 Authentication factors?

1. Something you know
   - One-time Password, Personal Identification Number (PIN), answer to a security question
2. Something you have
   - FOB, a hardware token, security key, and endpoint that can receive notification or text messages
3. Something you are
   - Biometrics, facial recognition etc.

When you combine two or more of the above it is now Multi-Factor Authentication

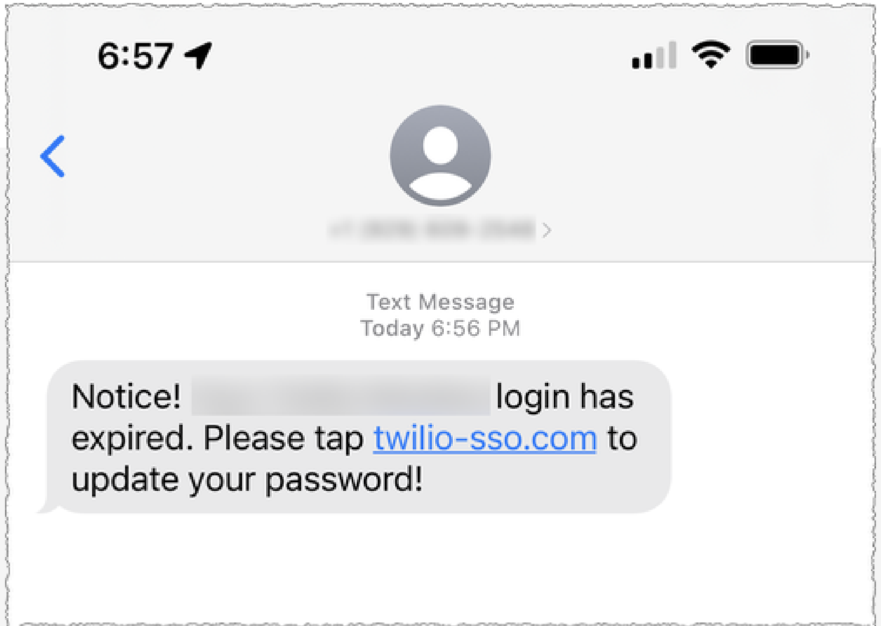
CrucialLogics
consulting with a conscience™

By-pass via Social Engineering

By-pass via Social Engineering

- As documented in the incident report **published by Twilio**; a limited number of Twilio customer accounts were compromised through a sophisticated social engineering attack designed to steal employee credentials.
- Hackers had done their reconnaissance and had the employees' username(s), first and last names and actual cellphone numbers.
- Attackers were impersonating Twilio's IT staff and sent text messages asking them to update the passwords.
- When people clicked on the link, they were presented with fake but authentic-looking landing pages.
- Twilio used a One-Time Password as the 2FA authentication mechanism.
- Users were asked to type in the One-Time Passwords that appeared on the authentication app which were used immediately to login into their actual accounts by the attackers.
- 125 Twilio customers whose data was accessed by malicious actors for a limited period of time, and Twilio has notified all of them,
- No evidence that customer passwords, authentication tokens, or API keys were accessed without authorization.

twilio

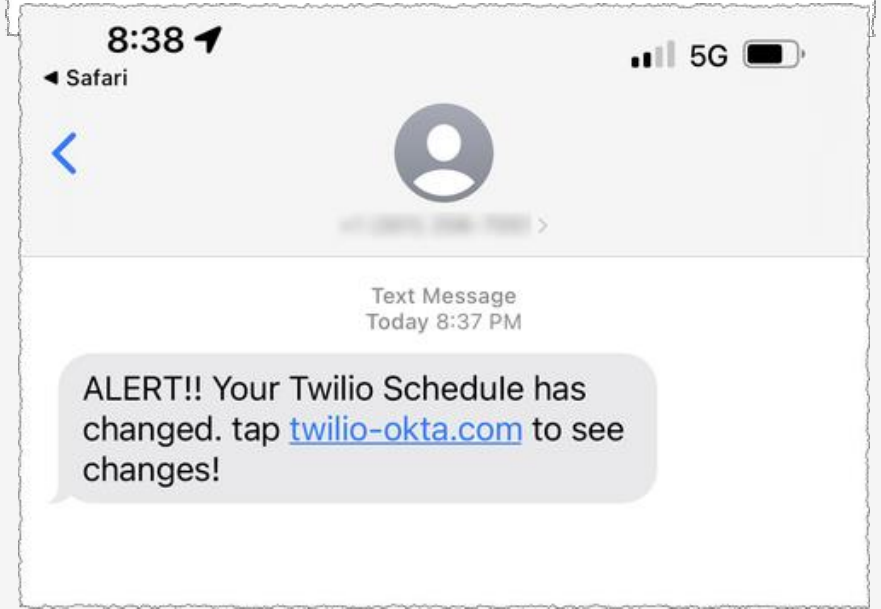


6:57

[redacted]

Text Message
Today 6:56 PM

Notice! [redacted] login has expired. Please tap twilio-sso.com to update your password!



8:38

[redacted]

Text Message
Today 8:37 PM

ALERT!! Your Twilio Schedule has changed. tap twilio-okta.com to see changes!

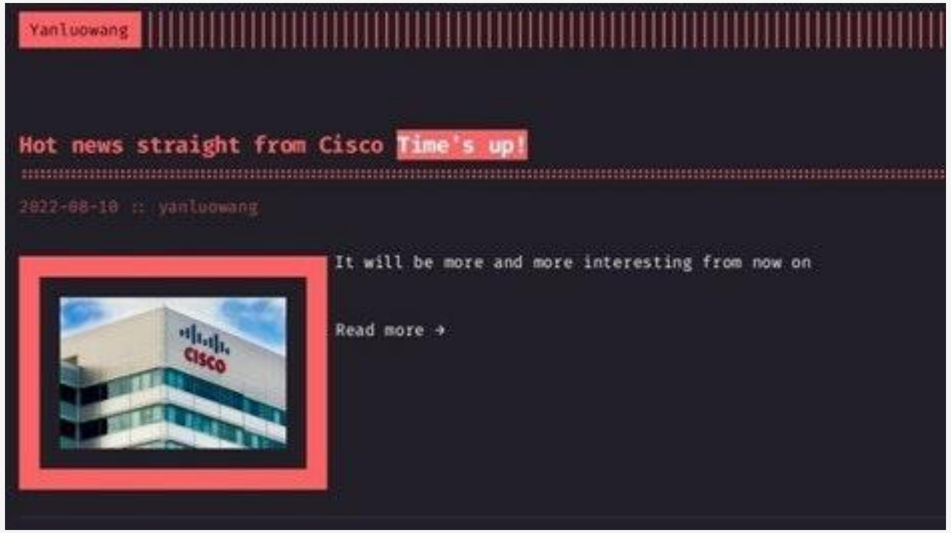
By-pass via MFA Fatigue

MFA by-pass via MFA Fatigue

In August 2022 Cisco confirmed that they had been breached by the Yanluowang ransomware group. Yanluowang group claimed that they had stolen 2.75 GB of Cisco data, consisting of 3100 files including NDA and Engineering documents.

How did this happen?

- Yanluowang gang compromised Cisco employee's personal Gmail account possibly through phishing, or the employee had been reusing passwords or the employee downloading credential-stealing malware.
- The employee was using a google password manager to store Cisco credentials.
- The attacker now had the Cisco Credentials but **required** MFA to authenticate to CISCO VPN.
- Below are the two techniques that were used to get past the MFA
  - Voice Phishing – Called the user pretending to be from the support organization
  - MFA Fatigue – Triggered MFA push notification repeatedly hoping the user would eventually approve to silence the constant notification
- The final step was to enroll their own device to simplify the future authentications
- Once Inside they established persistence using tools like LogMeIn & TeamViewer. Cobalt Strike and Mimikatz were then dropped for credential harvesting and lateral movement



Yanluowang

Hot news straight from Cisco Time's up!

2022-08-10 :: yanluowang

It will be more and more interesting from now on

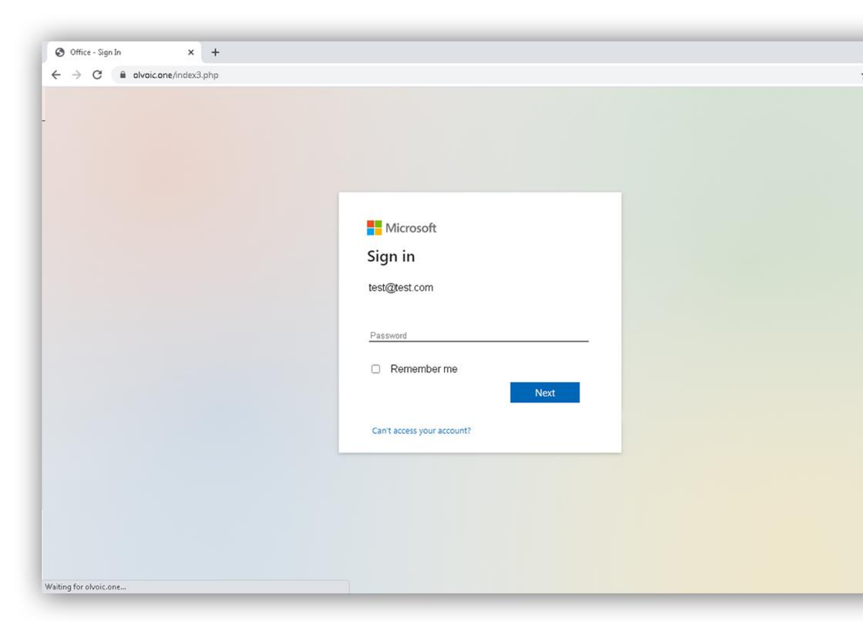
Read more →

By-pass via Session Hijacking

MFA by-pass via session hijacking

Tool called Evilginx is used which is a man-in-the-middle framework which allows bad actors to steal passwords.

The tool has templatized phishing pages which look similar to the authentic login page.



test@test.com

Password

□ Remember me

Next

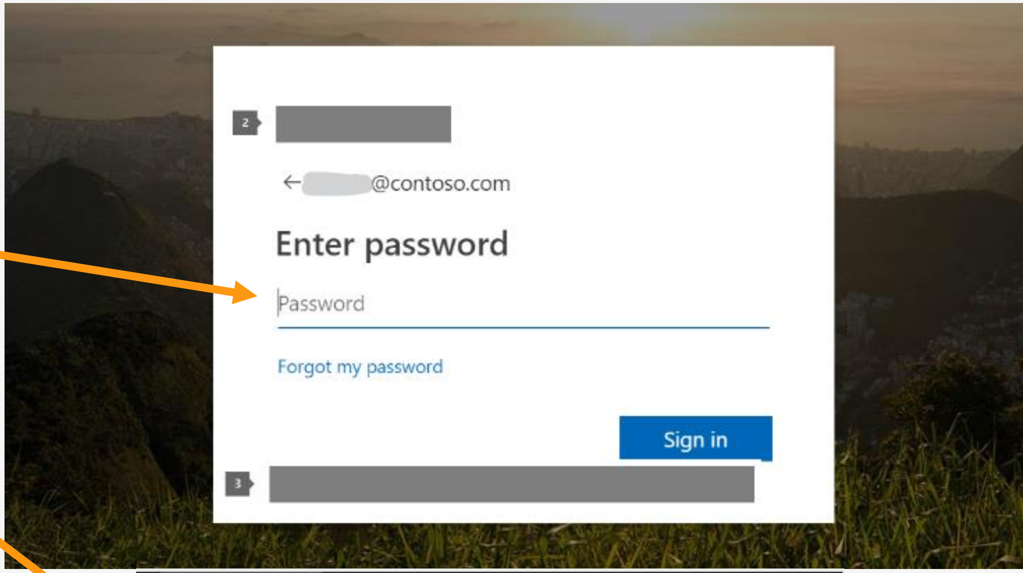
Can't access your account?

Waiting for olvoic.one...

Using common Social Engineering techniques users is tricked into clicking on the fake website and asking for a username.

MFA by-pass via session hijacking

The fake website will then proxy over to the real website for the password


2 [redacted]

← [redacted]@contoso.com

Enter password

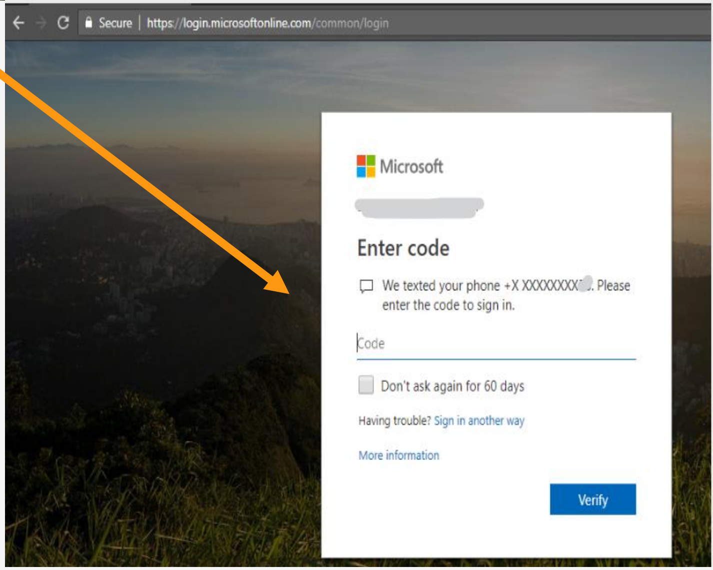
Password

Forgot my password

Sign in

3 [redacted]

Then the user is presented with MFA challenge. Users with SMS or One-Time-Passwords will get a code on their mobile phones and enter that code.



Microsoft

[redacted]

Enter code

We texted your phone +X XXXXXXXX[redacted]. Please enter the code to sign in.

Code

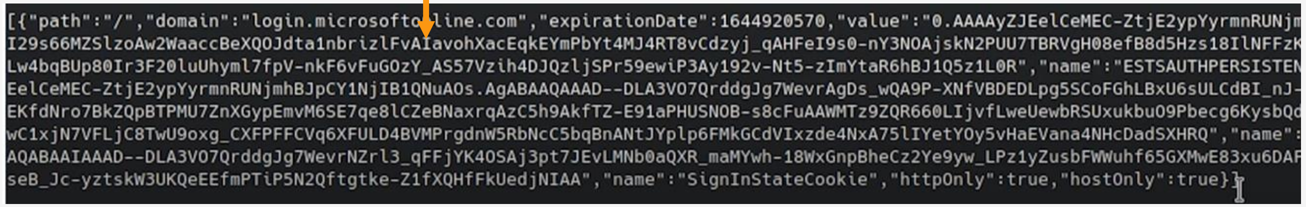
□ Don't ask again for 60 days

Having trouble? Sign in another way

More information

Verify

The attacker will intercept the session cookie via the proxied fake website.



```
[{"path":"/","domain":"login.microsoftonline.com","expirationDate":1644920570,"value":"0.AAAAyZJEelCeMEC-ZtjE2ypYyrmnRUNjm
I29s66MZSlzoAw2WaaccBeXQOJdta1nbrizlFvAIavohXacEqkEYmPbYt4MJ4RT8vCdzyj_qAHFeI9s0-nY3NOAjskN2PUU7TBRVgH08efB8d5Hzs18IlNFFzK
Lw4bqBUp80Ir3F20luUhyml7fpV-nkF6vFuGOzY_AS57Vzih4DJQzljSPr59ewiP3Ay192v-Nt5-zImYtaR6hBJ1Q5z1L0R","name":"ESTSAUTHPERSISTEN
EelCeMEC-ZtjE2ypYyrmnRUNjmhBJpCY1NjIB1QNuAOs.AgABAAQAAAD--DLA3VO7QrddgJg7WevrAgDs_wQA9P-XNfVBDEDLpg5SCoFGhLBxU6sULCdBI_nJ-
EKfdNro7BkZQpBTPMU7ZnXGypEmvM6SE7qe8lCZeBNaxrqAzC5h9AkfTZ-E91aPHUSNOB-s8cFuAAWMTz9ZQR660LIjvfLweUewbRSUxukbuO9Pbecg6KysbQd
wC1xjN7VFLjC8TwU9oxg_CXFPFFCVq6XFULD4BVMPrgdnW5RbNcC5bqBnANtJYplp6FMkGCdVIxzde4NxA75lIYetYOy5vHaEVana4NHcDadSXHRQ","name":
AQABAAIAAAD--DLA3VO7QrddgJg7WevrNZrl3_qFFjYK4OSAj3pt7JEvLMNb0aQXR_maMYwh-18WxGnpBheCz2Ye9yw_LPz1yZusbFWWuhf65GXMwE83xu6DAF
seB_Jc-yztskW3UKQeEEfmPTiP5N2Qftgtke-Z1fXQHfFkUedjNIAA","name":"SignInStateCookie","httpOnly":true,"hostOnly":true}]
```

The attacker then proceeds to the real login page, opens "Developer Tools" on the chrome browser, adds the session cookie in the console and hits the refresh button. This grants the attacker access to the site in question without being prompted for username or password.

CrucialLogics
consulting with a conscience™

CrucialLogics
consulting with a conscience™

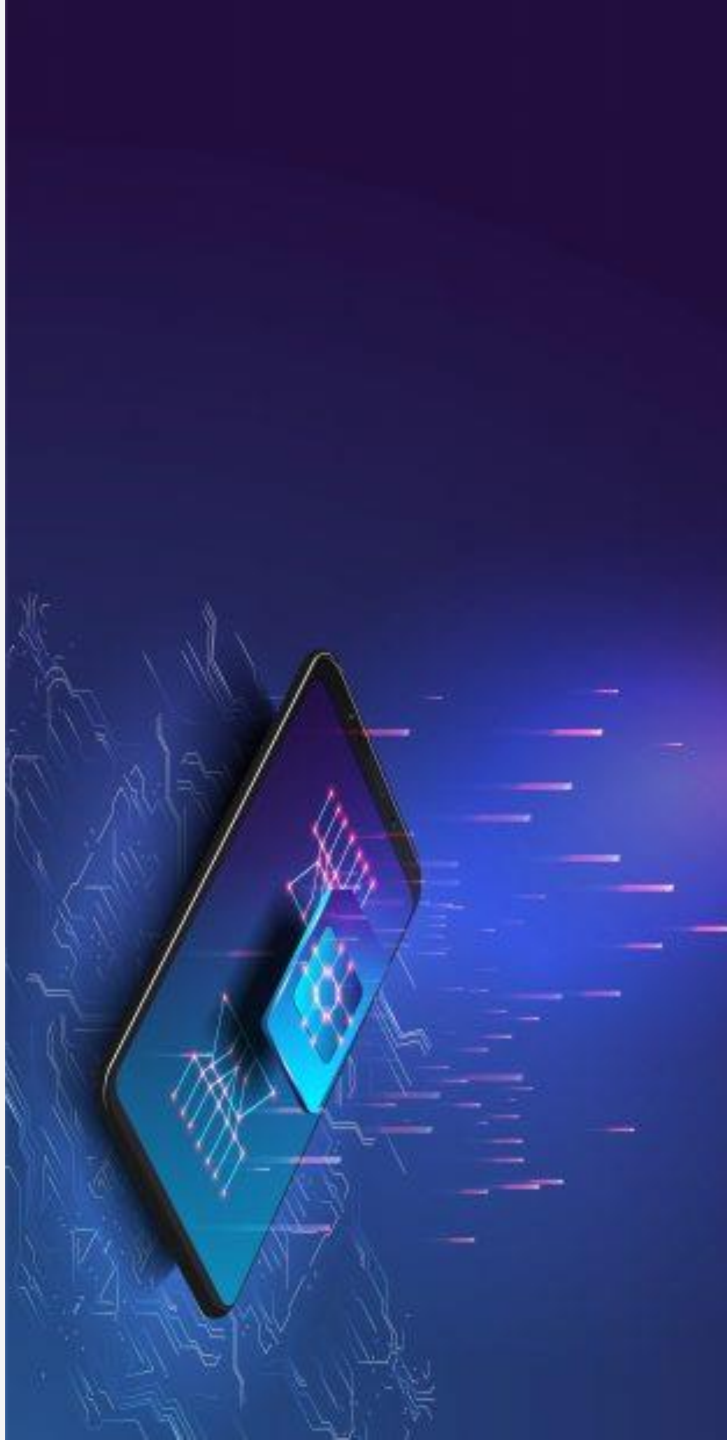
By-pass via SIM Jacking

MFA by-pass using SIM Jacking

Although relatively new SIM jacking is a type of identity theft that targets your phone number.

Manual Method:

1. Attackers can use SIM jacking to take over their cellphone accounts and gain access to your personal information, including text messages, contacts, and financial accounts.
2. If you use your phone number as one of the factors for authentication this can now be compromised
3. Attackers will text you pretending to be your carrier asking you to update your info by clicking on the link.
4. Your will then be taken to a fake website which mimics the carrier's website.
5. The website will ask you for all your personal information including cell your phone number and account pin
6. Then the attacker calls the carrier and asks to activate another SIM. This will then allow the attacker to intercept any 2FA codes sent via SMS and compromise the organization.



Common MFA Mistakes

On Feb 2022 – Microsoft made the following Statement

Despite years of promotional efforts to get users to enable stronger authentication mechanisms, Microsoft said that only 22% of all its Azure Active Directory (AD) customers used a multi-factor authentication solution to secure their accounts last year.

Why?

- Rolling out MFA requires proper design and planning
- It requires an understanding of the organization's authentication needs
- User devices, locations and ability has to be considered
- A badly designed MFA solution can just be a waste of time and money.
- Many organizations feel rolling out MFA is as simple as turning on the checkbox on the user's account. This cannot be farther from the truth

MFA considerations

- Organizational Change Management
- Documenting what assets and data the MFA solution will protect?
- What are the protocols used in the organization where MFA solution is being rolled out?
- How can these protocols be used to bypass MFA? (SMTP, IMAP, POP)
- Review of legacy systems that may fail once the organization adopts MFA for all its identities
- What form of MFA is required, authentication applications, or hard tokens?
- End-users and their ability to adopt new technology
- Do your users feel having a corporate application on your phone is an invasion of privacy?
- Do you need an HR policy around privacy and asking users to install a corporate-sponsored application?

How Can you prevent MFA bypass

- SMS form of second-factor authentication should be blocked immediately.
- Stop using One-time-password generated on MFA apps
- When asking users to authenticate on the second factor choose a solution that shows the location where the authentication request is coming from.
- Choose an authentication broker that supports authentication conditions such as geo-blocking or allows authentication only from specific IP ranges.
- Only allow access to corporate data from registered compliant devices.
- STOP users from accessing corporate data from home computers and unregistered phones.
- Harden your infrastructure so lateral movement is impossible

CrucialLogics
consulting with a conscience™

CrucialLogics
consulting with a conscience™

Final Defense!!

SECURITY AWARENESS TRAINING

Question…

☑ What MFA solution do you use in your organization?

Questions?

To ask a question,
type your question into the Chat located in the bottom right portion of the screen.

What's Next?

Take advantage of our experts to book an assessment, at no cost to you.

How To Get Started

- Book an appointment with one of our experts
- Download the additional information and resources in our follow-up email

Thank you for joining us today.

Amol Joshi
CrucialLogics
Amol.Joshi@cruciallogics.com