Exhibit F –

October 24 2023 Email ("October is Security Awareness Month")
Morning-of-termination correspondence with Nuvem's VP of IT Security Michael Larke and VP R&D Luigi Squillante, evidencing active, professional engagement moments before discharge. Rebuts any "attendance" pretext.

---------- Forwarded message ---------
From: **Albert Rojas** <arojas@nuvem.com>
Date: Tue, Oct 24, 2023 at 8:18AM
Subject: Re: October is Security Awareness Month
To: Michael Larke <mlarke@nuvem.com>
Cc: Luigi Squillante <Luigi@nuvem.com>

Sorry about that!

However, the Nuvem mail server did send me an alert that I am restricted emailing “all nuvem employees”. So that filter works.

But I am serious, it's all from the inside sir.

I have yet to see an enterprise breached from penetration. Only time the enterprise is breached is when the inside is sloppy:

1. leaving system-of-records on an edge mode for lightweight BI tools (Walmart, BofA)
2. IT releasing master keys to 3rd parties (TIAA Bank recent breach)
3. Data Policies not up to date (JPMC WhatsApp breach)

All that penetration does is point out which enterprise has yet to figure out virtual IP’s running servers as active/active (think Google 24/7)

I remember provisioning software for AMEX. The lead DBA escorted me into his walk-in bedroom closet, doing it all from a green screen CRT because even Jesus can’t get inside an AMEX Data center 😂

I learn everyday and excited learning more about the Nuvem process.

Respectfully,
Al Rojas

Get Outlook for iOS

Albert Rojas
Cloud Data Administrator

arojas@nuvem.com

nuvem
(Formerly 340Basics)
888-356-6225
www.nuvem.com

From: Michael Larke <mlarke@nuvem.com>
Sent: Tuesday, October 24, 2023 8:01:23 AM
To: Albert Rojas <arojas@nuvem.com>
Cc: Luigi Squillante <Luigi@nuvem.com>
Subject: Re: October is Security Awareness Month

Albert
Please do not reply to all on communications of this type.

Michael Larke
VP, IT Security, Compliance & Infrastructure

631-388-7192
mlarke@nuvem.com

nuvem
(Formerly 340Basics)
888-356-6225
www.nuvem.com

> On Oct 24, 2023, at 7:57 AM, Albert Rojas <arojas@nuvem.com> wrote:
>
> Yup, and while penetration monitoring is important, been there done that STIG-ing servers for national security… in my humble opinion, it all comes from the inside: www.OFAC.ai
>
> I wrote www.OFAC.ai during the lockdown after hearing stories that IBM Watson was trying to do the same and failing. It’s a global financial Bank off Broadway story and then some.
>
> “… **. Just like your housekeys, you want to do everything you can to keep your passwords safe…”**
>
> **Perhaps, but more important, you want to make sure you don’t leave your jewelry on the coffee table.**
>
> Excited to be at Nuvem (2nd week). And yes, the reverse train commute from the city is worth it, and then some. See attached exhibits.
>
> Respectfully,
> Al Rojas
>
> Get Outlook for iOS

Albert Rojas
Cloud Data
Administrator

arojas@nuvem.com

From: Michael Larke <mlarke@nuvem.com>
Sent: Tuesday, October 24, 2023 7:15 AM
To: All Nuvem Employees <All_Nuvem_Employees@nuvem.com>
Subject: October is Security Awareness Month

October is Security Awareness Month

Michael Larke
VP, IT Security, Compliance & Infrastructure

Did you know that October is Cyber Security Awareness Month?

Each week during the month of October, we will post topics with ways to protect the Company,

you and your family from cyber security risks & Threats

October 24, 2023

Phishing

Cybercriminals like to go phishing, but you don't have to take the bait.

Phishing is when criminals use fake emails, social media posts or direct messages with the goal of luring you to click on a bad link or download a malicious attachment. If you click on a phishing link or file, you can hand over your personal information to the cybercriminals. A phishing scheme can also install malware onto your device.

No need to fear your inbox, though. Fortunately, it's easy to avoid a scam email, but only once you know what to look for. With some knowledge, you can outsmart the phishers every day.

See it so you don't click it.

The signs can be subtle, but once you recognize a phishing attempt you can avoid falling for it. Before clicking any links or downloading attachments, take a few seconds (like literally 4 seconds) and ensure the email looks legit.

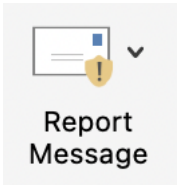
Here are some quick tips on how to clearly spot a phishing email:

- Does it contain an offer that's too good to be true?
- Does it include language that's urgent, alarming, or threatening?
- Is it poorly crafted writing riddled with misspel
- lings and bad grammar?
- Is the greeting ambiguous or very generic?
- Does it include requests to send personal information?
- Does it stress an urgency to click on an unfamiliar hyperlinks or attachment?
- Is it a strange or abrupt business request?
- Does the sender's e-mail address match the company it's coming from? Look for little misspellings like pavpal.com or anazon.com.

Uh oh! I see a phishing email. What do I do?

Don't worry, you've already done the hard part, which is recognizing that an email is fake and part of a criminal's phishing expedition.

If you're at the office and the email came to your work email address, click on the Report Message icon in the ICON menu of the message:



If the email came to your personal email address, don't do what it says. Do not click on any links – even the unsubscribe link – or reply back to the email. Just use that delete button. Remember, DON'T CLICK ON LINKS, JUST DELETE.

You can take your protection a step further and block the sending address from your email program.

Here's how to…

- Block a sender on Outlook.
- Block a sender on Gmail.
- Block a sender on Mac Mail.
- Block a sender on Yahoo! Mail

Report phishing.

Some email platforms let you report phishing attempts. If you suspect an email is phishing for your information, it's best to report it quickly. If the phishing message came to your work email, let your IT department know about the situation ASAP.

Here's how to:

- Report a phish on Outlook.
- Report a phish on Gmail.
- Report a phish on Mac Mail.

October 19, 2023

Software Updates

One of the easiest ways to boost your cybersecurity is to always keep software and apps updated.

Every day, software and app developers focus on keeping their users and products secure. They're constantly looking for clues that hackers are trying to break into their systems, or they are searching for holes where cybercriminals could sneak in, even if they've never been breached before. To fix these issues and improve security for everyone who uses their services, upstanding software companies release regular updates.

If you install the latest updates for devices, software, and apps, not only are you getting the best security available, but you also ensure that you get access to the latest features and upgrades. However, you can only benefit if you update! Don't fret, updating software is easy, and you can even make it automatic.

Here are four easy-to-remember tips to keep in mind when it comes to updates:

1. AUTOMATIC UPDATES MAKE YOUR LIFE EASIER

You don't have to check your Settings tab every morning – you can usually set up automatic updates so that updates are downloaded and installed as soon as they are available from the device, software, or app creator. Note that you might have to restart your device for the updates to fully install. It is best to do this right away, but you can often schedule this to happen during times when you aren't using your device, like the middle of the night. Plenty of us stay lazy and secure –although you probably should check your software update settings every so often (quarterly is good) to ensure everything is set to your liking!

2. SELECT FARM-RAISED UPDATES FRESH FROM THE SOURCE

Before downloading anything, especially software and app updates, be sure you know the source. Only download software to your computer from verified sources, and only download apps from your device's official app store. The device, software, or app developer itself should be sending you updates, not anyone else. And remember, pirated, hacked, or unlicensed software can often spread malware, viruses, or other cybersecurity nightmares to your network. Ruining your computer, phone, tablet, or other device isn't worth it!

3. DON'T FALL FOR PHISHY FAKES!

On the web, you've probably come across suspicious pop-up windows that urgently demand you download a software update. These are especially common on shady websites or if there is malware already on your machine. These are always fake – they are attempts at phishing. Don't click any buttons on these pop-ups and close your browser. Many web browsers will warn you if you are attempting to visit an unsecure web address or one that could contain malware. Heed these warnings and don't take the bait!

4. TURN CHECKING FOR UPDATES INTO A HABIT

Even if you don't have automatic software updates turned on, make updating your device, software, and apps a regular habit. Oftentimes, you will be notified that updates are available. Even if it is a pain to close out of your programs and restart your device, it is worth it to do this right away, especially if the update patches an urgent security flaw. You should check your app and device settings on a regular basis, and you should check monthly if you don't have automatic updates turned on (although weekly is better). Remember that updates are part of our digital lifecycle, and if you embrace them, you'll have more peace of mind, the latest security, and the best new features!

Update your devices and software with these direct links:

Operating Systems

- Android
- Chrome OS
- Apple
- Samsung
- Windows

Connected Devices

- Amazon devices (Fire Tablets, Kindle E-readers, Alexa Devices, Fire TV)
- Apple Watch
- Fitbit devices
- Garmin devices
- Google Nest or Home speakers
- Ring doorbells

October 10, 2023

Passwords are the keys to your digital castle. Just like your housekeys, you want to do everything you can to keep your passwords safe.

Passwords can be made ironclad with additional authentication methods, such as [multifactor authentication (MFA).]

Creating, storing and remembering passwords can be a pain for all of us online, but the truth is that passwords are your first line of defense against cybercriminals and data breaches. Also, it has never been easier to maintain your passwords with free, simple-to-use password managers. With a few moments of forethought today, you can stay safe online for years to come.

LONG, UNIQUE, COMPLEX

No matter what accounts they protect, all passwords should be created with these three guiding principles in mind:

- Long – Every one of your passwords should be at least 12 characters long.
- Unique – Each account needs to be protected with its own unique password. Never reuse passwords. This way, if one of your accounts is compromised, your other accounts remain secured. We're talking really unique, not just changing one character or adding a "2" at the end – to really trick up hackers, none of your passwords should look alike.
- Complex – Each unique password should be a combination of upper case letters, lower case letters, numbers and special characters (like >,!?). Again, remember each password should be at least 12 characters long. Some websites and apps will even let you include spaces.

HOW OFTEN DO I CHANGE MY PASSWORD?

If your password is long, unique and complex, our recommendation is that you don't need to ever change it unless you become aware that an unauthorized person is accessing that account, or the password was compromised in a data breach.

This recommendation is backed up by the latest guidance from the National Institute of Standards and Technology. For many years, cybersecurity experts told us to change our passwords every few months. However, this constant change isn't helpful if your passwords are each long, unique and complex. In fact, if you change your passwords often, you risk reusing old passwords or falling into bad habits of creating similar or weak passwords.

BUT REMEMBERING ALL MY PASSWORDS IS SO HARD!?

You probably have a lot of online accounts. And because all your passwords should be unique, that means you have a lot of passwords. But the fact remains that using long, unique and complex passwords remains the best way to keep all of your digital accounts safe. There are many free and easy-to-use tools out today that makes managing your library of unique passwords a snap.

Today, the truth is that you don't have to remember your passwords. If you use the latest tools, you don't need to rack your brain at every login screen. You just need to remember the one password that unlocks your password manager vault.

DON'T TAKE A PASS ON PASSWORD MANAGERS.

As our lives expand while we do more online, we've gone from having just a couple of passwords to today, where we might manage upwards of 100 or more. If you're like most people, you're probably using the same password for most of your accounts—and that's not safe. If your one password gets stolen because of a breach, it can be used it to gain access to all your accounts and your sensitive information. But no need to fret, password managers are easy to use and make a big difference. ssword managers are easy to use and make a big difference.

Learn more about password managers

October 2, 2023

Multi-factor authentication allows you to protect yourself in multiple ways

Wouldn't it be nice if you could protect your password with another password? Multi-factor authentication gives you this power – think of it like placing your housekeys in a safety deposit box that can only be opened by a facial scan. In some cases, this metaphor isn't far off from reality.

What is multi-factor authentication?

Multi-factor authentication is sometimes called two-factor authentication or two-step verification, and it is often abbreviated to MFA. No matter what you call it, multi-factor authentication is a cybersecurity measure for an account that requires anyone logging in to prove their identity multiple ways. Typically, you will enter your username, password, and then prove your identity some other way, like with a fingerprint or by responding to a text message.

Why go through all this trouble? Because multi-factor authentication makes it extremely hard for hackers to access your online accounts, *even if they know your password*.

It might seem like a lot of work, but once you have multi-factor authentication set up, proving your identity usually adds just a second or two to the log-in process. And the peace of mind multi-factor authentication provides is well worth it.

We recommend that you implement multi-factor authentication for any account that permits it, especially any account associated with work, school, email, banking, and social media.

How does multi-factor authentication work?

When you turn multi-factor authentication on for an account or device, your log-in process will require a bit more verification.

You will be asked for your username and password.

If these are correct, you will then be prompted to prove your identity another way. You might be able to set up your smartphone, for example, to use a facial scan as verification. Other online accounts might send your phone number or email address a one-time use code that you must enter within a certain frame of time. Some accounts will require you to approve access with a standalone authenticator app like Duo or Google Authenticator.

Different forms of multi-factor authentication

Multi-factor authentication can take several different forms, including:

- Inputting an extra PIN (personal identification number) as well as your password
- The answer to an extra security question like “What town did you go to high school in?”
- A code sent to your email or texted to your device that you must enter within a short span of time
- Biometric identifiers like facial recognition or fingerprint scan
- A standalone app that requires you to approve each attempt to access an account
- An additional code either emailed to an account or texted to a mobile number
- A secure token – a separate piece of physical hardware, like a key fob, that verifies a person’s identity with a database or system

What type of accounts offer multi-factor authentication?

Not every account and device offers multi-factor authentication, but it is becoming more common every day. You might already have it set up for your devices, like if you use a Face ID or fingerprint scan to unlock your phone or laptop. multi-factor authentication is now often found in many workplaces and universities, too.

Here are some types of accounts that often offer multi-factor authentication. Check to see if you can turn multi-factor authentication on:

- Banking
- Email
- Social media
- Online stores

Multi-factor authentication adds an entire layer of security on your important accounts beyond your password. Your data is precious and important – multiplying its protection is a great idea. Let’s use multi-factor authentication everywhere!

Can multi-factor authentication be hacked?

While multi-factor authentication is one of the best ways to secure your accounts, there have been instances where cybercriminals have gotten around multi-factor authentication. However, these situations typically involve a hacker seeking multi-factor authentication approval to access an account multiple times and the owner approving the log-in, either due to confusion or annoyance.

Therefore, if you are receiving multi-factor authentication log-in requests and you aren't trying to log in, *do not approve the requests!* Instead, contact the service or platform right away. Change your password for the account ASAP. Also, if you reused that password, change it for any other account that uses it (this is why every password should be unique).

Don't let this deter you, though. multi-factor authentication is typically very safe, and it is one of the best ways you can bolster the security of your data!

View in SharePoint

Michael Larke
VP, IT Security, Compliance & Infrastructure

631-388-7192
mlarke@nuvem.com

<nuvem-finalregisted-highres-smallsize_3668769a-5169-48e8-a72b-a94fa97a34e0.png>

(Formerly 340Basics)
888-356-6225
www.nuvem.com