



# SAFE COMPUTING

CS101- ONION CREEK SENIOR CENTER

Mike O'Donnell

Website: <https://safe-computing.net>

Email: [mike@safe-computing.net](mailto:mike@safe-computing.net)

Phone: 512-228-0411

Safe Computing

# Safe Computing - Agenda

1

Introduction

2

Getting started

3

Let's spin the wheel!!

4

Five common sense tips to be safe?

5

Q&A and final survey

# Mike O'Donnell

Information Technology (IT) Director – Retired  
Semiconductor Industry – 1994 to 2022

Owner of the ***Safe Computing*** consulting business  
that is facilitating this class today.

(See: <https://safe-computing.net>)

**Safe Computing** – this class is intended to create  
awareness of the potential risks of internet usage and to  
give recommendations how to stay secure.



# Course Objectives

1. Have fun learning something you will hopefully find interesting.
2. Leave with a better understanding of the risks of internet usage and how to avoid them.

Please do not be afraid to stop and ask questions or ask for help. Sometimes things don't work or maybe the instructions are not clear or the information you typed in was incorrect. It's Ok to make mistakes or not understand something, so please ask questions. That's how we really learn!

Need help? Just contact the Help Desk!!!!



That's Me!

# Safe Computing - Agenda

1

Introduction

2

Getting started

3

Let's spin the wheel!!

4

Common sense tips to be safe?

5

Q&A and final survey

# Getting Started.... First Things First!

## **Repeat:**

Please do not be afraid to stop and ask questions or ask for help. Sometimes things don't work or maybe the instructions are not clear or the information you typed in was incorrect. It's Ok to make mistakes or not understand something, so please ask questions. That's how we really learn!

## **Student/Group ID Number:**

Everyone will get a "Student ID" number. Every table has been numbered as well. We will use this during this class.

## **Class Survey:**

At the end of the class, we hope that you will please take a bit of time to complete the class survey. It let's us know what you thought of the class and the instructor so we can make it better.

# Safe Computing - Agenda

1

Introduction

2

Getting started

3

Let's spin the wheel!!

4

Common sense tips to be safe?

5

Q&A and final survey

*And what wheel is that?*







**WALLET BEFORE**

- 1.Face book Logins
- 2.Credit Card Details
- 3.Email Account Logins
- 4.Photos and documents

You must contact us immediately so we can walk you through the removal process to protect your identity. Please call us to prevent your computer from being damaged and information loss.

**Toll Free: +1-888-619-2111**

**WALLET AFTER**

+1-888-619-2111

Your day is just beginning with a cup of coffee and some Facebook. Your sister-in-law sends you a message with an attachment. You click it and...

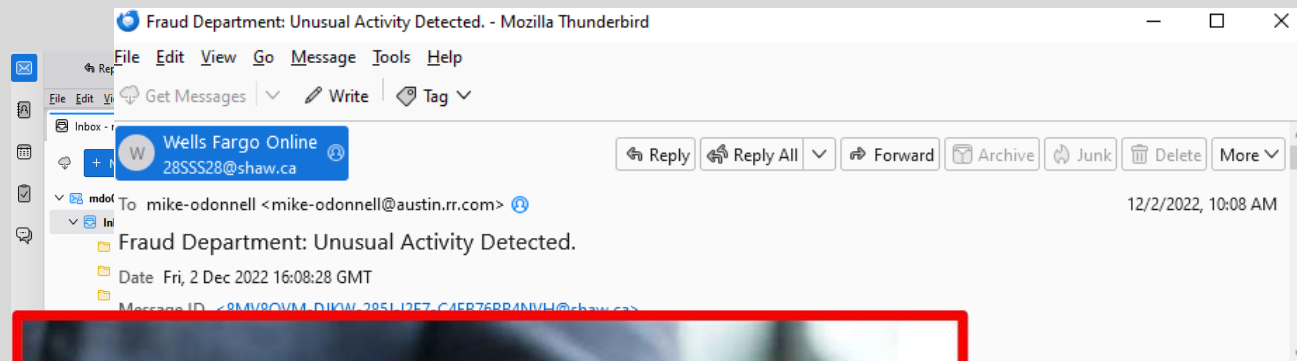
Oh My, the infamous **MS-SYSINFO32** error pops up on your screen!!! What do you do now????

**This warning is fake. How to remove and resolve this issue:**

- DON'T CALL Microsoft!
- Restart your computer
- Log in and run free malware removal tools such as:
  - MalwareBytes
  - Spybots Search & Destroy
  - AdwCleaner
  - Your anti-virus file scanner

<https://malwaretips.com/blogs/remove-error-ms-sysinfo32>





**WALLET BEFORE**

Thank you for choosing WellsFargo.

Please do not reply to this automated email. If you have any questions please log in to online banking and use the Secure Message Service to send a secure message.

©2021 WellsFargo Bank. All rights reserved.



**WALLET AFTER**

Your day is just beginning with a cup of coffee and catching up on some email.

Uh-oh.... a **FRAUD** alert from your Wells Fargo bank account!!!! Ouch! What do you do now????

**This email is fake. How did I know? How**

[shaw.ca](http://shaw.ca)

at is very, very old  
account  
g" like goes to  
t

ward  
g into  
mber, but that

end of the message

- What to do? Delete this email.

'mdo0911  
info\_MXODMMYQIK@newsurpuhngsntmu.edu

To mdo0911@gmail.com

Cc mdo0911@gmail.com

confirmation#4835534

Date Mon, 05 Dec 2022 17:51:56 +0100

Message ID <YDQWUWVYVGO-Ct-A2WK2RPWYX-@dvdc.dcccd.edu>

Bank of America  
21ss5321ss5321wop1alerts@shaw.ca

To mike-odonnell <mike-odonnell@austin.rr.com>

An Update on Your Online Profile

Date Tue, 19 Mar 2024 12:21:53 +0100

Message ID <IW0VFMXZ-M4M1-JME1-R4NX-73511JGQQOUJ@shaw.ca>

Return-Path <21ss4521ss4521wop1alerts@shaw.ca>

Reply Reply All Forward Archive Junk

iCloud Storage  
info@ultramiko.hunoghund.com

To mdo0911@gmail.com

mdo0911 :Congrats! You've received an iCloud Storage Bonus ID#8094

Date Mon, 25 Mar 2024 21:41:29 +0000.70-86596

Message ID <p7xcu4kg65o0qiz96b0@sailthru.com>

Return-Path <return@ultramiko.hunoghund.com>

Reply Forward Archive Junk Delete More

AVG: Message body was removed because it contained a virus.

compte sur inscription-Facile votre compte a ete cree, mais

Thanks for asking. There's a "forgot password" link on the l

In addition to that, there are a couple other options on the

Failure to follow the instruction may result in a temporary hold!





**WALLET BEFORE**



**WALLET AFTER**

Your day is just beginning with a cup of coffee, and you decide to browse some vacation photos you just took.

Uh-oh, a popup appears on your screen informing you that **“your files have been encrypted”!!!**

What do you do now???

**How to remove and resolve this issue:**

**NEVER PAY THE RANSOM!**

Identify your ransomware strain  
Uninstall the ransomware if possible

- Establish a proactive defense

<https://www.safetydetectives.com/blog/how-to-solve-oops-your-files-have-been-encrypted-in>





**WALLET BEFORE**

| <a href="#">View Transactions</a> <a href="#">View Statement</a> <a href="#">Print</a> |        |
|----------------------------------------------------------------------------------------|--------|
| CARD                                                                                   | AMOUNT |
| Michael O. ...1177                                                                     | \$9.19 |



**WALLET AFTER**

Your day is just beginning with a cup of coffee and a review of your credit card expenditures, which you had just learned was important.

You notice a couple of charges that you know you didn't make! And you realize this is the only card that was sent to you.

What do you do?

How did this happen?

**How to resolve this issue:**

1. Contact your credit card company and report the fraud. Have the card cancelled and get a new one.  
2. Update any auto-pay you might have setup.

Hackers often breach businesses and steal credit card information, or a skimmer is installed on a card reader such as a gas pump. Then it is sold on the "Dark Web"

← → ↺ 🔒 https://onionengine.com/search.php?search=credit+card&submit=Search&rt=

27921 results found !

Help Onion Search Engine, [MAKE A DONATION](#) or [BUY ME A COFFEE](#).

---

 [Best shop card,cards, cloned cards, credit card, visa card, buy card, prepaid card, shop cards, debi](#)  
<http://7f5zddtszyf3sgmv7wnt3peu5mwfpwbnmrk3w7pimnjiz7q3acydyd.onion/>  
Best shop card,cards, cloned cards, credit card, visa card, buy card, prepaid card, shop cards,  
debit card buy store cc.clone@dnmx.org Home Delivery Question/An...  
 [Online](#) |  [Report abuse](#) | [Tor2Web](#)

---

 [Best shop card,cards, cloned cards, credit card, visa card, buy card, prepaid card, shop cards, debi](#)  
<http://63pl2uefkf2ssznscxiaa23s2tvrsmmnghwtgdkxx633ptoqn3d77hid.onion/>  
Best shop card,cards, cloned cards, credit card, visa card, buy card, prepaid card, shop cards,  
debit card buy store cc.clone@skiff.com Home Delivery Question/A...  
 [Online](#) |  [Report abuse](#) | [Tor2Web](#)

---

 [Best shop card,cards, cloned cards, credit card, visa card, buy card, prepaid card, shop cards, debi](#)  
<http://cd2lludn15f2qeltzrx3pp2izkdfycy2pyolvxrsgunk4qgthrskkad.onion/>  
> Best shop card,cards, cloned cards, credit card, visa card, buy card, prepaid card, shop cards,  
debit card buy store cc.clone@dnmx.org Cart(0) Home Delivery Q...  
 [Online](#) |  [Report abuse](#) | [Tor2Web](#)

---

AD SPACE AVAILABLE

728X90

Click Her for more info

 [by Traffic Juicy](#)

---

 [snovmarket – sell credit cards – Credit cards for you. big sale credit cards](#)  
<http://xsqpuzf3p2oap6yzyjyhhroobbmlmuulvxhho5o5tf2axxf6xwgoj3cyd.onion/>  
snovmarket – sell credit cards – Credit cards for you. big sale credit cards Skip to  
content Home My account Orders Checkout Cards Credit cards Prepaid card...  
 [Online](#) |  [Report abuse](#) | [Tor2Web](#)

---

 [Card & Wallet Shop - Dumps PayPal & Dumps Credit Card & Bitcoin Wallets - Shop hacked PayPal account](#)  
<http://irt54zixqahseagg6onsaaimpliufiprawsqk5mxo2eegeubj2ktqlqd.onion/>  
Card & Wallet Shop - Dumps PayPal & Dumps Credit Card & Bitcoin Wallets - Shop hacked PayPal

A simple search of the “dark web” reveals people selling stolen credit card information.

Criminals buy credit card numbers in batches. They then simply “burn” the credit card information on programmable cards just like those used for hotel room access.





**WALLET BEFORE**



**WALLET AFTER**

Your day is just beginning with a cup of coffee and your cheerful submission of your IRS income tax form using TurboTax. You are done (again) and begin the "eFile" process....

But Oh, No, it got **REJECTED!!!**

What do you do?

How did this happen?

**How to resolve this issue:**

Use IRS Form 14039 to alert the IRS that someone has filed a return using your identification. The IRS may send you a "[Letter 5071C](#)" asking that you verify your identity. You can respond via telephone or through the IRS' online [Identity Verification Service](#).

<https://turbotax.intuit.com/tax-tips/security/identity-theft-what-to-do-if-someone-has-already-filed-taxes-using-your-social-security-number/L4NBQHS2>





**WALLET BEFORE**



**WALLET AFTER**

One day you wake up to a good cup of coffee and some time reading your emails, browse social media and just get your day started as usual. But....

It soon you realize that this is not the usual start to the day. In your Inbox is an email with the subject line that asks, "Give me your password 'abc123'". Whoa! 'abc123' is one of your passwords and so you take the instructions to read this seriously. What do you do?

**What to do:**

Find the account using the "abc123" password and change it  
Then do NOTHING

<https://www.myantispysware.com/2024/02/07/i-recorded-you-email-scam-what-to-do-if-youre-targeted>





**WALLET BEFORE**



**WALLET AFTER**

One day you wake up to a good cup of coffee and begin work on lodging for your upcoming vacation to London in three months! You find an incredible flat near all the sites for a fraction of what other rentals cost. You initiate a dialog with the landlord and agree on your travel dates with plans to stay seven days. Total price: £560 (about \$450 USD) Next, to seal the deal, he asks

sent via Western Union that must be from the reservation.

or payment and follow up with an en sent. The landlord replies with a that you should contact him just the check-in instructions.

days away. As instructed you check-in instructions.

ur email but not reply....

rived. You check your email once ly. What do you do?

### What to do?

- Realize you have been scammed
- Report it to Western Union
- NEVER send money to someone you don't know via Western Union!



# The BIG day has come!!!! You are flying to London!!!

uploaded in HD @ TunesToTube.com



**WALLET BEFORE**



**WALLET AFTER**

Unfortunately, your jet plane doesn't leave for another two hours. So, you decide to open your laptop to check your bank account and take care of some other business. You connect to the free airport WiFi and you are off to internet races!

Time has arrived. You close your laptop, grab your carry-ons and enjoy the most relaxing week in London. But..... Uh-oh!

When you get back home and start catching up on work, you find your bank account drained, credit cards maxed, and your Facebook hacked!!! What happened? What to do?

If you are a victim of using unprotected, public WiFi, even if you take specific measures, your data can still be seen by hackers in the same waiting area.

- Make sure to always connect to web services using the 'https' (not 'http') protocol
- Consider getting a VPN product which encrypts your internet connection. VPN is also recommended to use from home

# Safe Computing - Agenda

1

Introduction

2

Getting started

3

Let's spin the wheel!!

4

Common sense tips to be safe?

5

Q&A and final survey

# Safe Computing

We just learned about a lot of ways hackers can exploit innocent people.

*What you don't know can hurt you.*

Please. **DO NOT BE SCARED**

The intent of this class was not to scare you, but to educate.

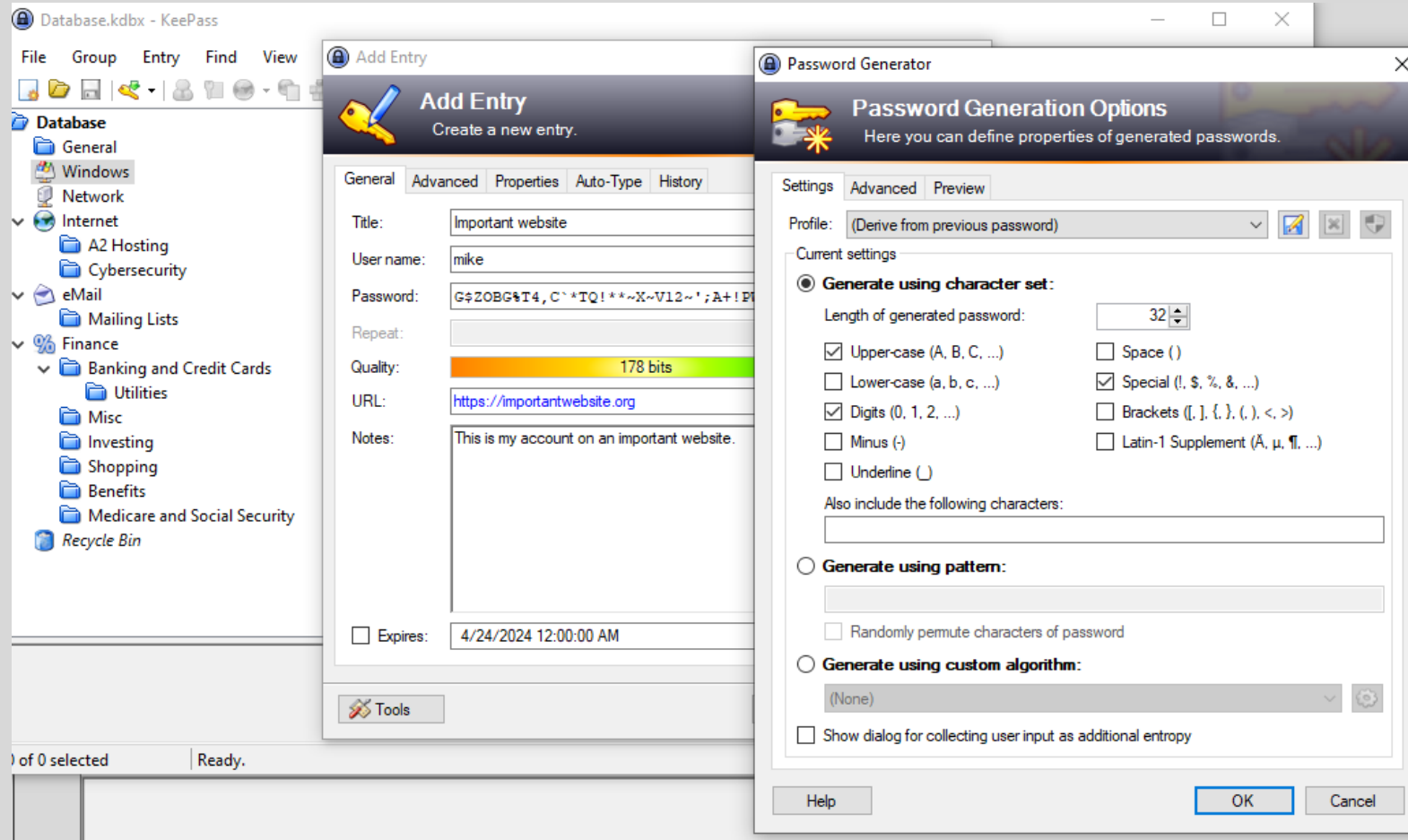
Now that you are more aware of the risks, there are some simple suggestions that will help you be safe.

## 1. Implement good password management processes

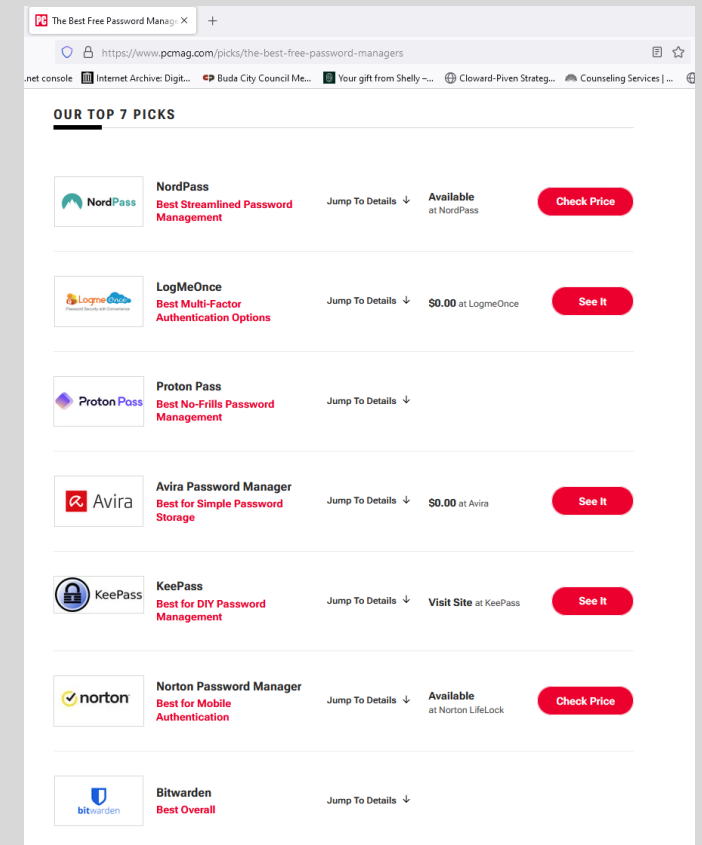


# 1. Implement good password management processes

Use a good password manager (vault).



## Free Password Managers



1. Implement good password management processes
2. **Limit what data you share online, or in person (credit card or bank info, social security number or any personal information)**



**WATCH THIS HACKER  
BREAK INTO  
MY CELL PHONE ACCOUNT  
IN 2 MINUTES**

1. Implement good password management processes.
2. Limit what data you share online (credit card or bank info, social security number and personal information).
- 3. Make sure your anti-virus software is working.**
- 4. If it's too good to be true, then it probably is.**
- 5. Don't click on links or attachments in emails from people you don't know**
- 6. Don't use public wifi if possible, use VPN if you must.**

1. Implement good password management processes.
2. Limit what data you share online (credit card or bank info, social security number and personal information).
3. Make sure your anti-virus software is working.
4. If it's too good to be true, then it probably is.
5. Don't click on links or attachments in emails from people you don't know
6. Don't use public wifi if possible, use VPN if you must.
7. **Monitor your accounts. Set alerts at low thresholds (e.g. credit card) that will email and/or text you when activity takes place. Set alerts to be sent when your accounts are logged into.**





 3 Steps to



**Step 1** Protect yours to generate and save each website.

## 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.



**Cit0day (unverified):** In November 2020, a collection of more than 23,000 allegedly breached websites known as Cit0day were made available for download on several hacking forums. The data consisted of 226M unique email address alongside password pairs, often represented as both password hashes and the cracked, plain text versions. Independent verification of the data established it contains many legitimate, previously undisclosed breaches. The data was provided to HIBP by [dehashed.com](#).

**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



**Houzz:** In mid-2018, the housing design website Houzz suffered a data breach. The company learned of the incident later that year then disclosed it to impacted members in February 2019. Almost 49 million unique email addresses were in the breach alongside names, IP addresses, geographic locations and either salted hashes of passwords or links to social media profiles used to authenticate to the service. The data was provided to HIBP by [dehashed.com](#).

**Compromised data:** Email addresses, Geographic locations, IP addresses, Names, Passwords, Social media profiles, Usernames



**Ticketfly:** In May 2018, the website for the ticket distribution service Ticketfly was defaced by an attacker and was subsequently taken offline. The attacker allegedly requested a ransom to share details of the vulnerability with Ticketfly but did not receive a reply and subsequently posted the breached data online to a publicly accessible location. The data included over 26 million unique email addresses along with names, physical addresses and phone numbers. Whilst there were no passwords in the publicly leaked data, [Ticketfly later issued an incident update](#) and stated that "It is possible, however, that hashed values of password credentials could have been accessed".

**Compromised data:** Email addresses, Names, Phone numbers, Physical addresses

y number

v

at will  
when your

## What to do?

If your account(s) have been breached, then change your passwords immediately!

1. Implement good password management processes.
2. Limit what data you share online (credit card or bank info, social security number and personal information).
3. Make sure your anti-virus software is working.
4. If it's too good to be true, then it probably is.
5. Don't click on links or attachments in emails from people you don't know
6. Don't use public wifi if possible, use VPN if you must.
7. Monitor your accounts. Set alerts at low thresholds (e.g. credit card) that will email and/or text you when activity takes place. Set alerts to be sent when your accounts are logged into.
8. Check if your accounts have been compromised.
  1. <https://haveibeenpwned.com/>
9. **DON'T PANIC!!!!**

**This slide deck can be downloaded from:**

**<https://mdo-web301/sched/CS101-OCSC.pdf>**



# Safe Computing - Agenda

1

Introduction

2

Getting started

3

Let's spin the wheel!!

4

Common sense tips to be safe?

5

Q&A, a surprise and the final survey

A woman with long dark hair, wearing a blue top, a grey cardigan, and light-colored trousers, stands in a long aisle of a server room. She is reaching out to touch a server rack on the right. The racks are filled with blue cables and green indicator lights. The room has a high ceiling with a grid of lights and a tiled floor. In the background, red numbers 4, 5, and 6 are visible on the wall.

# Q&A



# Addendum