CSU Connection
Serving our community for over 30 years
June 2023

Our mission is to deliver outstanding IT support to your business in order to improve uptime, productivity. and profitability.

You take care of running your business, we'll take care of your technology.

in this issue...

Quote of the Month

"Someone is sitting in the shade today, because someone planted a tree a long time ago."

-Warren Buffet

Is it Time to Ditch the Passwords for More Secure Passkeys?

Passwords are the most used method of authentication, but they are also one of the weakest. Passwords are often easy to guess or steal. Also, many people use the same password across several accounts. This makes them vulnerable to cyber-attacks.

The sheer volume of passwords that people need to remember is large. This leads to habits that make it easier for criminals to breach passwords, such as creating weak passwords and storing passwords in a non-secure way.

61% of all data breaches involve stolen or hacked login credentials.

In recent years a better solution has emerged – passkeys. Passkeys are more secure than passwords. They also provide a more convenient way of logging into your accounts.

Passkeys work by generating a unique code for each login attempt. This code is then validated by the server. The code is created using a combination of information about the user and the device they are using to log in.

You can think of passkeys as a digital credential. A passkey allows someone to authenticate in a web service or a cloud-based account. There is no need to enter a username and password.

This authentication technology leverages Web Authentication (WebAuthn). This is a core component of FIDO2, an authentication protocol. Instead of using a unique password, it uses public-key cryptography for user verification.

The user's device stores the authentication key. This can be a computer, mobile device, or security key device. It is then used by sites that have passkeys enabled to log the user in.

Advantages of Using Passkeys Instead of Passwords:

More Secure

One advantage of passkeys is that they are more secure than passwords. Passkeys are more difficult to hack. This is true especially if the key generates from a combination of biometric and device data.

Biometric data can include things like facial recognition or fingerprint scans.

cont. on pg 2

Device information can include things like the device's MAC address or location.

This makes it much harder for hackers to gain access to your accounts.

More Convenient

Another advantage of passkeys over passwords is that they are more convenient. With password authentication, users often must remember many complex passwords. This can be difficult and time-consuming.

Forgetting passwords is common and doing a reset can slow an employee down. Each time a person has to reset their password, it takes an average of three minutes and 46 seconds.

Passkeys erase this problem by providing a single code. You can use that same code across all your accounts. This makes it much easier to log in to your accounts.

It also reduces the likelihood of forgetting or misplacing your password.

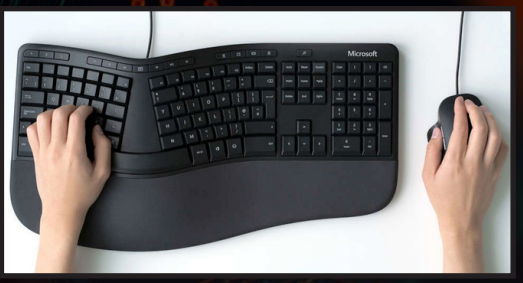
Phishing-Resistant

Credential phishing scams are prevalent. Scammers send emails that tell a user something is wrong with their account.

They click on a link that takes them to a disguised login page created to steal their username and password.

When a user is authenticating with a passkey instead, this won't work on them. Even if a hacker had a user's password, it wouldn't matter. They would need the device passkey authentication to breach the account.

[Business] Gadget of the Month



Wrist strain is a common problem for regular keyboard users.
Ergonomic keyboards are nothing very new, but this latest offer from Microsoft moves things forward with the addition of more programmable 'favorites', a dedicated emoji button, and lots of customization options to boost your productivity!

(And it doesn't break the bank at around $50)

Get yours today at Amazon.com or Best Buy

Tech Facts

Did you know?

1. 48% of malicious email attachments use Microsoft Office file extensions, disguised as an invoice or receipt
2. 43% of employees don't know that clicking a suspicious link or opening an unknown attachment could lead to malware infection
3. 1 in 3 employees don't believe there is a security risk in failing to password-protect their devices

Password Managers *Explained:*

-What is a password manager?

A password manager is software that generates, stores, and syncs login credentials across multiple devices. There are many options available, each with slightly different features and price-points.

-How does it work?

Password managers store your credentials behind one master password that unlocks the software. To log into an account, you simply enter your password and the software does the rest. Whenever you set up a new online account, the manager can automatically generate a strong unique password for that account, and save it on your behalf.

Most password managers will automatically fill online login forms with the click of a button. They can also store personal information (such as your name, address, phone number, email, etc.) and payment options (such as credit card data), and automatically fill that information as needed.

Should you use a password manager at work?

Simple answer: follow policy. Some organizations use password managers while others don't. Never install any unapproved software on work devices.

-Should you use one in your personal life?

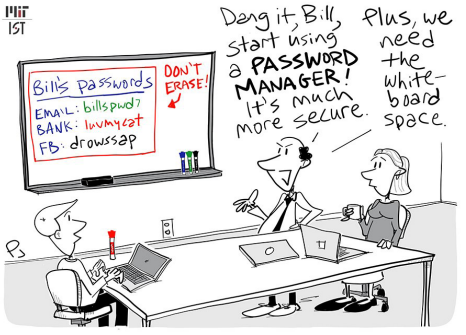
Generally speaking, yes. It's nearly impossible for most of us to remember the dozens and dozens of login credentials we need every day.
Password managers solve this problem by requiring you to remember only a single, master password.

-Are password managers secure?

There are two schools of thought to consider. On the downside, password managers could be viewed as a single point of failure. It stores every login credential you give it access to. If the developer gets hacked, it could mean that all of your passwords get exposed in a single breach. Big yikes. This has happened in the past, but is extremely rare.

On the upside, password managers remove the hassle of creating and remembering strong passwords. This reduces the use of inferior or weak passwords and solves the issue of password storage.

Most security professionals agree that the rewards outweigh the risks.



How To Stay Safe on Social Media: A Series

Our social media apps are part of our lives and like any convenient tool (think email, your smart phone and car) they need to be managed and mastered. Every day brings new challenges to your safety and security.

Here are some of the ways to keep yourself **protected and secure:**

1. ***Treat your personal info like cash*** *and think hard before you give it away*

2. ***Check your settings.*** *Even if the social media app isn't asking you for data, assume that it is collecting it with your implied acceptance. Mark your mobile device settings (Camera, Microphone, Location, Sync contacts) to OFF until they are needed for that function and then reset the default to OFF.*

3. ***Enable MFA (Multi-factor authentication also known as 2 factor authentication.*** It makes it hard for hackers to access your online accounts, even if they know your passwords.

4. ***Use long, strong and unique passwords.***

5. ***Share with Care!*** *The more information that you post, the easier it is for hackers to steal your identity and commit other crimes. Think who you allow to see your personal posts; most platforms allow you to limit who can see or engage with you.*

6. ***THINK BEFORE YOU POST!*** *Posts stay around forever and may come back to haunt you!*

7. ***Think twice before accepting a request or invitation to connect from just anyone.*** *Many social media networks have tools that allow you to manage the info you share with friends in different groups.*

(continued on pg 5)

Part 1: Facebook and LinkedIn

Facebook

With almost 3 Billion users, Facebook is the most used social media app. Of course, it comes with dangers. It's easy to be scammed when everything looks so friendly and nice! Go to Facebook.com/help and adjust your settings under Privacy, Safety and Security for some of the security measures you may not know about:
Under Security Features and Tips, get alerts when someone tries to login to your account.
Under Your Privacy: Adjust who can see your Friends section and set to your comfort level
Under Control who can see what you share on Facebook: use the audience selector to pick who you want to see the post. You can also change who it's shared with after posting.

Also watch for:
- Account related scams
- Free stuff from third parties
- Disaster relief and other charity scams
- Curiosity Traps

LinkedIn

Considered the "Business" social media app, LinkedIn still has many traps. Along with the usual scam (romance, crypto investment, etc) employment scams are rampant! Once you apply, the recruiter asks you for personal data, such as your Social Security number (SSN), bank account information, or a credit report.

Here's what to look for:
•Be suspicious of unsolicited job pitches that seem too good to be true. If any offer piques your interest, verify that it's a legitimate opening by looking on the company's official website.
•When submitting a resume, only disclose publicly available information. Don't share details like your phone number, address, or identification numbers.
•Beware of employers who do "text-only" interviews, especially on encrypted chat apps like WhatsApp or Telegram.
•Never buy a credit report to share with an employer.
Any job that requests this is a scam.

Happy Birthday to the one and only, the starter of it all... Chuck Sherman!

32 Years ago, Chuck had the idea and ambition to start his own computer IT company. Now here we are!
As founder and CIO of CSU, Chuck is an overall **awesome, knowledgable**, and **hardworking** person who is just plain good at what he does!
He is an amazing coach and boss! His jokes and tenacity set him apart from the rest, and ensure that there is never a boring day at the office!

Happy 60th Birthday Chuck!! We appreciate all that you do so much!
And so do our CSU clients :) ~

"The most memorable thing about Chuck is his demeanor. No matter how ramped up the client is about their IT problem, Chuck is **cool and collected** with his response to the situation and his explanation on how the issue will be resolved. For me, **it always put my worries to rest..."**
-Dr. Bollenback with Towne Animal Clinic

"Chuck **saved the day** for us before we were even clients – **that is what made us clients!**"
-Becky from PUMC

"Chuck has managed the complexity of Caring Hands and its owner structure, and is always calm, cool, and collected. Thank you for your **great guidance!**
-Dr. Vitulli with Caring Hands Animal Hospital

"Happy Birthday to Chuck! He's always on top of things and willing to help.....
Chuck took to the task like the pro that he is, and we never missed a beat. There is a certain comfort in knowing that, no matter what the issue is, Chuck is always on-call ready to take care of it!"
-Bass with Akina Pharmacy

A little bit about Chuck...

Chuck's favorite movie: *50 First Dates*
"I'm a huge Adam Sandler fan." He once watched it *three times in a row* (with his daughter of course).

Chuck's dream vacation:
"If I were 20 years younger and flights were better priced, I'd go all across the US and Europe. My only rule is *No Weird Food*!" He also would enjoy an Alaskan cruise.

If Chuck competed in the Olympics, it'd be for ***soccer***.

If Chuck could be on any gameshow, it would be ***Family Feud***!

Making a Difference...

World Vision

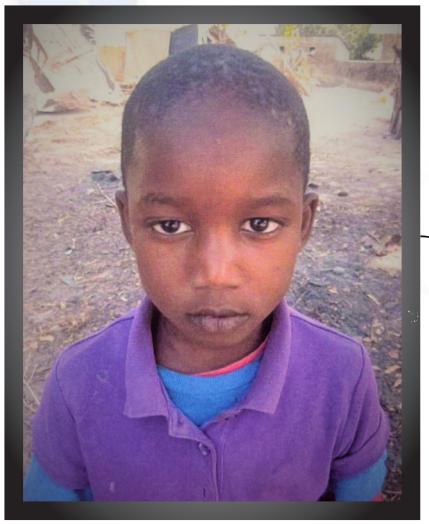
This month, CSU has decided to partner with World Vision, a Christian humanitarian organization who helps children, families, and communities overcome poverty, to sponsor two children in Africa by making monthly donations to support the mission of those working hard to foster support, growth, and a future for these children's lives.

If you are interested in sponsoring a child or learning more, go to www.myworldvision.org

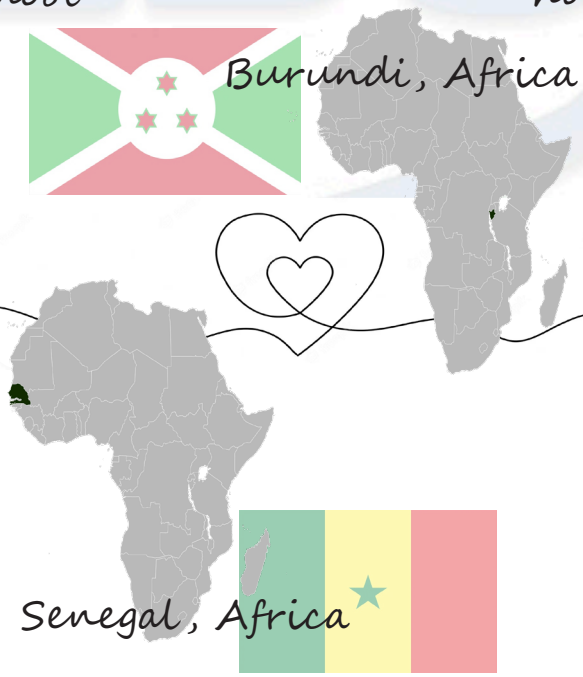
Meet Thierno and Sifa!

Thierno is a 6 year old boy who lives in Oussouye, Senegal, Africa. He lives with his parents, one brother, and two sisters. Both his father and mother are unemployed and find it difficult to meet their family's needs.

Thierno says that he likes to play soccer, and that his favorite part about school is coloring!

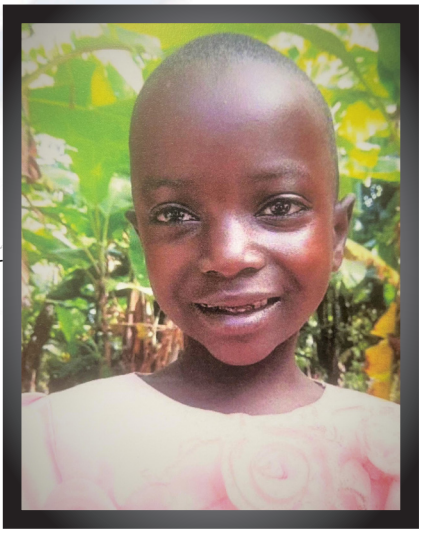


Thierno



Sifa is a 5 year old girl who lives in Butezi, Burundi, Africa. She lives with her parents, who are both farm laborers, and her one sister. Despite their efforts, they find it difficult to meet the family's needs.

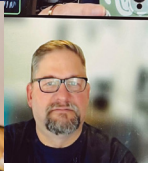
Sifa says that she likes to play ball games and helps at home by doing chores!



Sifa

What's Happening at CSU?

We decided to play a lit-tle prank on Melvin.... or do we mean, Marvin!



After getting to know Melvin, a suave and witty guy, it's easy to get such a unique name mixed up with another, such as "Marvin".

Everyone at CSU began slowly catching on to this new trend and as each day passed, his pet name of endearment began to stick!

Until the day that we received a ticket from a client with the title.....

Help Marvin!

...that was the moment it all came together! They had no idea!

We sent "Marvin" to pick up pizza, and he returned to an unexpected surprise.

His reaction (and laugh) were priceless.

Melvin is an awesome tech, caring friend, and a true jokester.

Now, he has a shirt and can proudly bear his name wherever he goes :)

Did you know the 3rd Friday in May is National Pizza Party Day?