

Administrative Office of the Courts – 2025 ACAP Systems Conference

Cybersecurity Basics: Keep Calm and Change Your Password

July 23-25, 2025



Cybersecurity Events

Kansas Courts

October 12, 2023

Foreign actor breached state's online case management system

Stole case records and judicial administration files

Threatened to post data on the dark web if demands weren't met

Impact

Case management system down for 3 months

File exfiltration investigation lasted 7 months

Kansas court officials confirm details of 'evil, criminal' international cyberattack

Preliminary assessment indicates information stolen for use on dark web

BY: TIM CARPENTER - NOVEMBER 21, 2023 1:47 PM



Kansas Supreme Court Chief Justice Marla Luckert and the six associate justices issued a statement Tuesday that said the Oct. 12 information system attack was perpetrated by sophisticated foreign criminals who stole information and threatened to post it to the dark web if demands weren't met. (Pool photo by Evert Nelson/Topeka Capital-Journal)

Kansas Courts

May 6, 2024

Office of Judicial Administration announced findings

Exfiltrated data affected 150,000 citizens

Breached data included:

- SS#s
- Driver's Licenses
- Payment Card Info
- Passport Numbers
- Health Insurance Policy Information
- Biometric Identifier

Kansas court investigation confirms cyberattack compromised personal data of 150K people

BY: RACHEL MIPRO - MAY 6, 2024 4:19 PM



Chief Justice Marla Luckert said the Kansas Supreme Court prioritized storing data securely and has implemented more data security controls since the breach. (Sherman Smith/Kansas Reflector)

<https://kansasreflector.com/briefs/kansas-court-investigation-confirms-cyberattack-compromised-personal-data-of-150k-people/>

Cybersecurity Events

L.A. County

July 19, 2024

LA County Courts suffered a ransomware attack

Impact

All 36 courthouses

Impacted court website, jury system, case management system

Los Angeles Times

CALIFORNIA

Devastating ransomware attack shuts down L.A. County courts.
All courthouses to reopen Tuesday



The Stanley Mosk Courthouse in downtown Los Angeles was closed Monday after a ransomware attack, which officials said did not appear to be related to the CrowdStrike software update that paralyzed computers around the world last week. (Kent Nishimura / Los Angeles Times)

AOC - Linda

Attack

Successful phishing attack from a breached account.

Victim allowed MFA bypass.

From: Carol Jenkins <cjenkins@cscdcaa.org>
Sent: Thursday, September 14, 2023 8:25 AM
To: Linda Hamilton <linda.hamilton@arcourts.gov>
Subject: FYI- Please Find Attached Essential Information On Behalf Of Crawford-Sebastian Community Development Council, Inc.
Importance: High



CAROL JENKINS HAS SHARED A SECURE DOCUMENT WITH YOU

Recipient: linda.hamilton@arcourts.gov

Ref Number: 00197397

File Type: Pdf

VIEW.

One Microsoft Way, Redmond, WA 98052, USA



Carol Jenkins
Crawford-Sebastian Community Development Council, Inc.
Deputy Director/Li-HEAP Director/Child Care Food Program Director
479-945-2303 ext. 212
479-250-4602
1617 S. Zero
Fort Smith, AR 72901

AOC - Linda

Impact

Attacker sent phishing emails to 1926 address book entries.

Statistically – 15-46 additional victims.

From: Linda Hamilton <linda.hamilton@arcourts.gov>
Sent: Friday, September 15, 2023 6:42 AM
To: Brett Watson <watson@bdwpllc.com>
Subject: FYI- Please Find Attached Essential Information On Behalf Of Arkansas Judiciary
Importance: High



LINDA HAMILTON HAS SHARE A SECURED DOCUMENT WITH YOU

Intended Recipient: watson@bdwpllc.com

Ref Number: 0018797

File Type: Pdf

VIEW.

One Microsoft Way, Redmond, WA 98052, USA



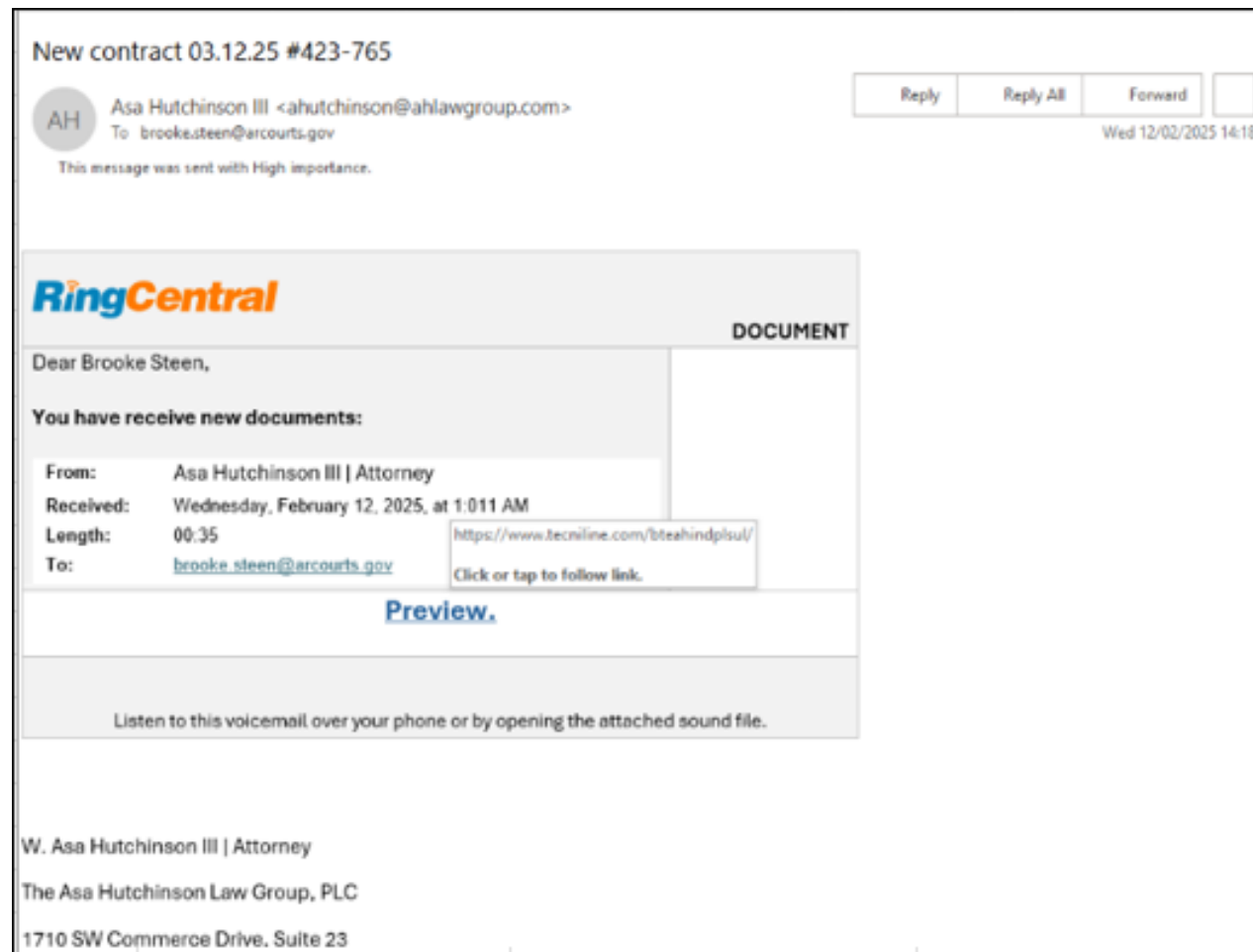
Thank you.

Respectfully,
Linda Hamilton

AOC - Brooke

Attack

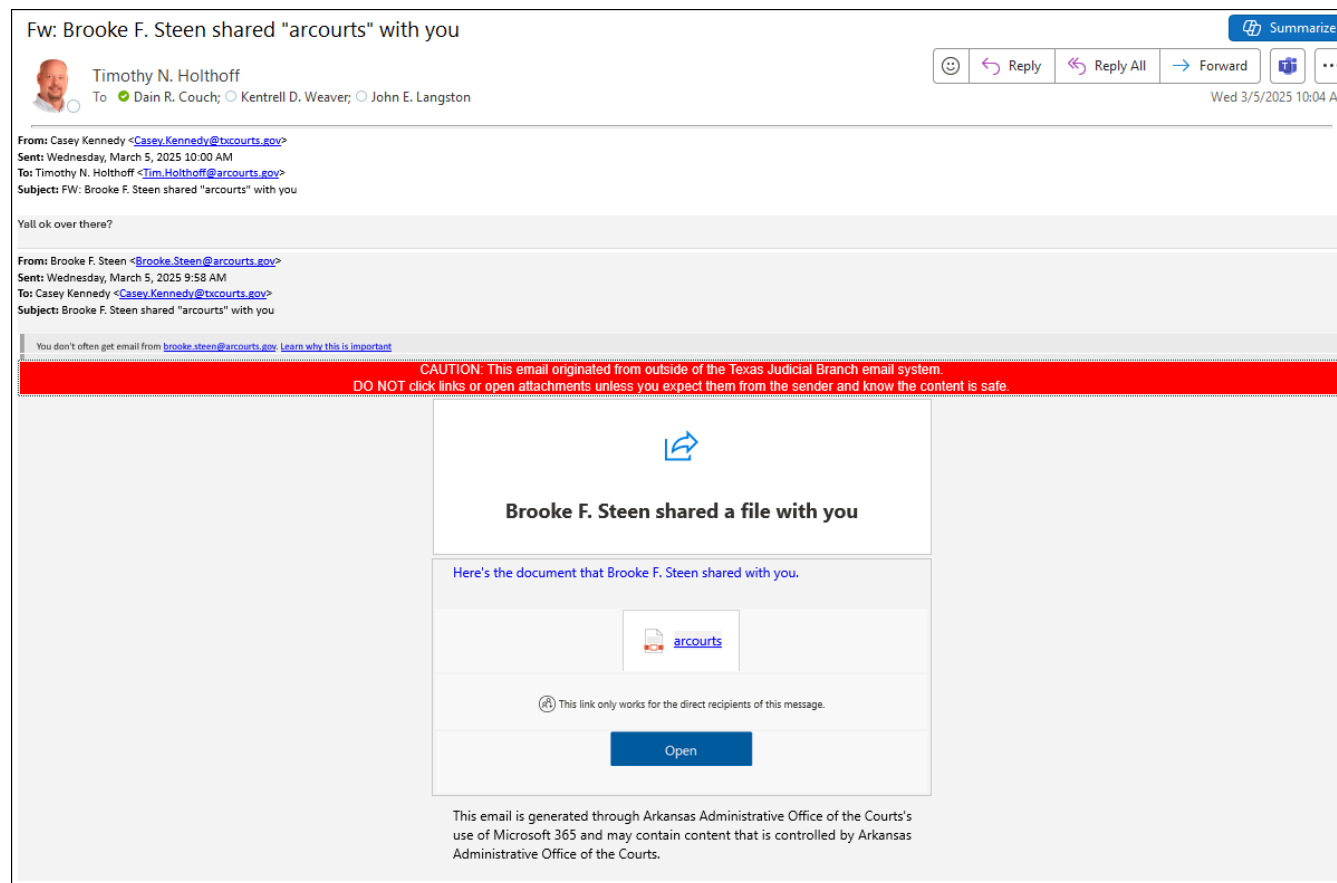
- Attacker stole session token
- Established foothold
- Copied email box
- Added malicious document
“arcourts.pdf”
- Emailed 795 addresses



AOC - Brooke

Impact

- Statistically 8-24 additional victims.
- At least 1 judge and 1 clerk clicked and entered their credentials.
- Clerk paycheck rerouted to attacker.
- Information for possible future attacks.



Hackers

HACKERS

Who is hacking?

Script Kiddies

Knowledgeable Users

Hactivists

State Actors

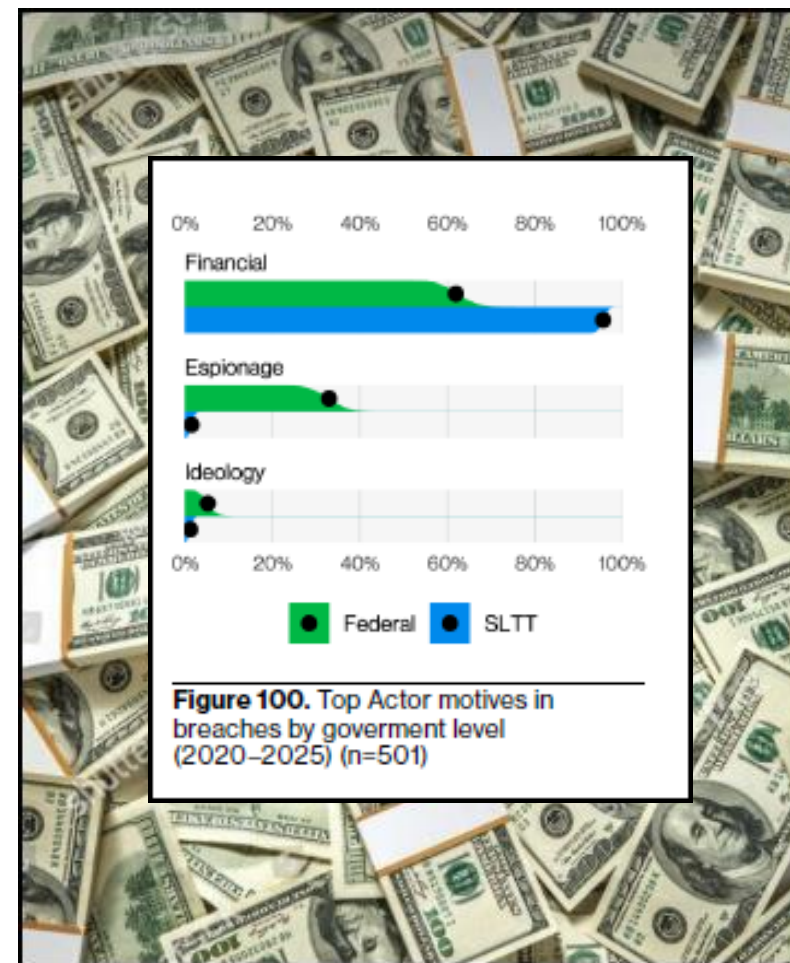
Organized Crime



What do they want?

For state and local government, it's about money.

96% of breaches for state and local governments were financially motivated in 2024.



HACKERS

“I don’t have anything.”

**Access to a system/network
is all a hacker needs.**

HACKERS

What Can you do to protect court data?

Software Updates

Malicious Emails

Artificial Intelligence

Passwords

Multifactor Authentication (MFA)

Password Managers

Key Takeaways

Don't click on stuff

Choose a good password

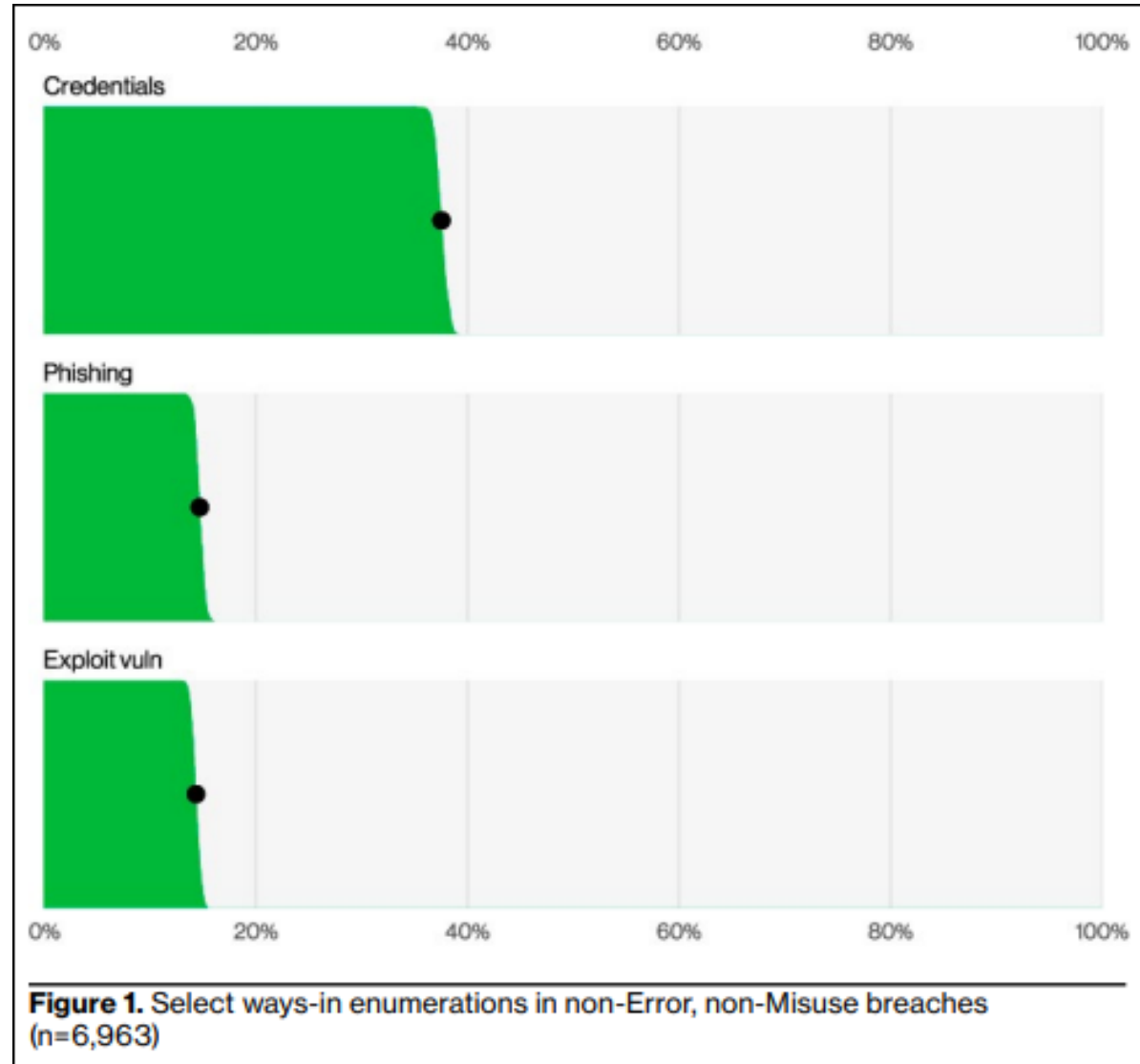
Software Updates

SOFTWARE UPDATES

Organizational Updates

IT Departments should be scanning for missing updates and updating computers.

- 18% of breaches stemmed from vulnerabilities
- Almost 3 times as many as 2022!



2024 Verizon Data Breach Investigations Report

SOFTWARE UPDATES

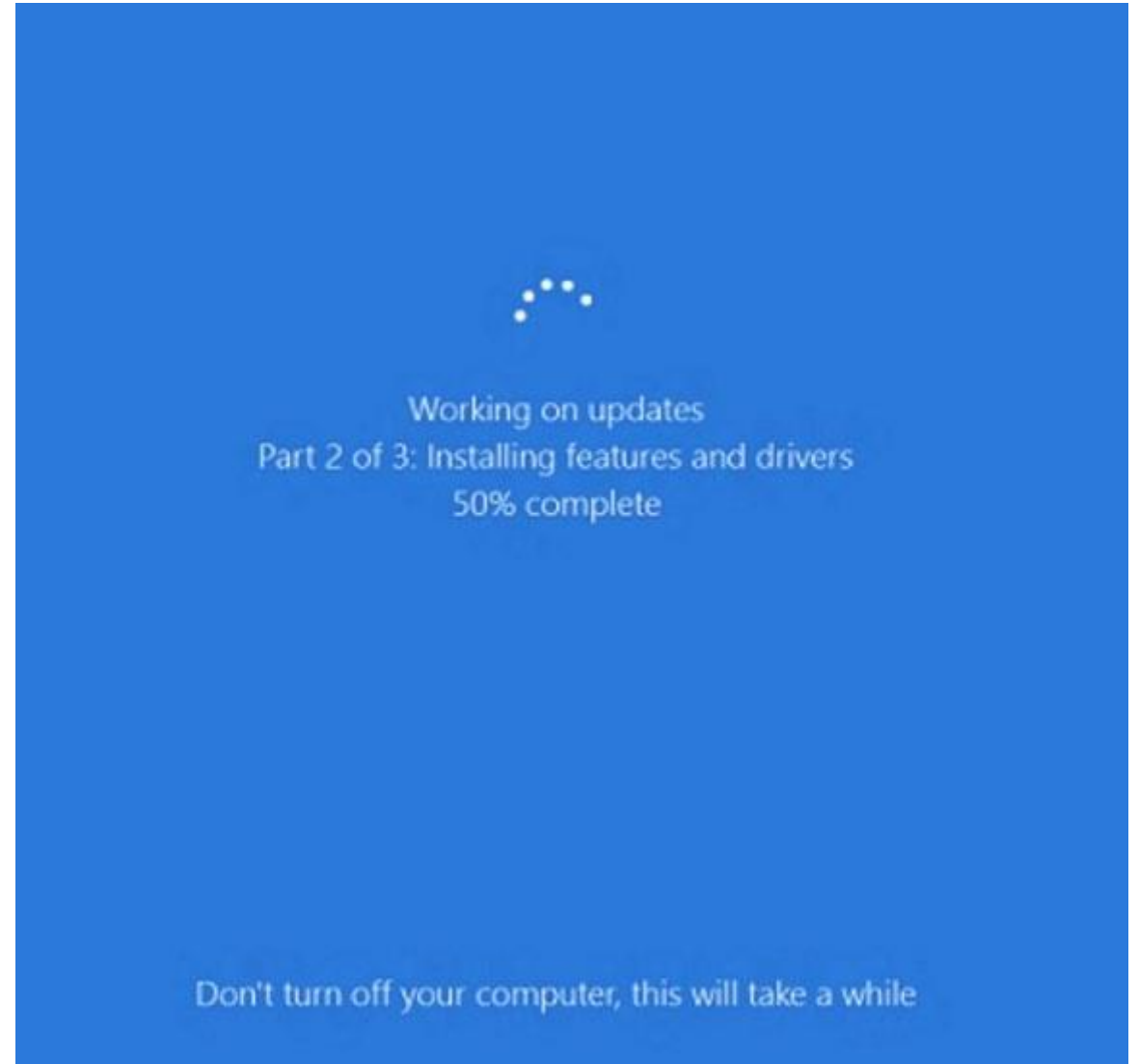
Purpose of Updates

Updates help software run better, add new features, and correct security flaws

Tips

Set software to update automatically

*Keep in mind that updates may require a restart to install.



Malicious Emails

The Threat

2024

4.3% of Public Sector breaches were attributed to phishing emails.

2020

70% of Public Sector breaches were attributed to phishing emails.

2026

Could be 70% again! This depends on tactics but phishing effectiveness has not decreased.



Identifying Malicious Emails

- Try to convince you to click on a link or attachment.
- You do not know the sender and/or the email address is long/convoluted/strange.
- Word usage/grammar/punctuation errors.
- Email details that do not apply to you (package tracking, airline ticket, court/legal proceedings, etc.).

Can result in loss of credentials or malware (including ransomware).

Artificial Intelligence is making malicious emails more effective.

PHISHING/MALICIOUS EMAILS

Example Email

From: Carol Jenkins <cjenkins@cscdcaa.org>
Sent: Thursday, September 14, 2023 8:25 AM
To: Linda Hamilton <linda.hamilton@arcourts.gov>
Subject: FYI- Please Find Attached Essential Information On Behalf Of Crawford-Sebastian Community Development Council, Inc.
Importance: High



CAROL JENKINS HAS SHARED A SECURE DOCUMENT WITH YOU

Recipient: linda.hamilton@arcourts.gov

Ref Number: 00197397

File Type: Pdf

VIEW.

One Microsoft Way, Redmond, WA 98052, USA



Carol Jenkins
Crawford-Sebastian Community Development Council, Inc.
Deputy Director/Li-HEAP Director/Child Care Food Program Director
479-945-2303 ext. 212
479-250-4602
1617 S. Zero
Fort Smith, AR 72901

PHISHING/MALICIOUS EMAILS

Example Email

From: Carol Jenkins <cjenkins@cscdcca.org>
Sent: Thursday, September 14, 2023 8:25 AM
To: Linda Hamilton <linda.hamilton@arcourts.gov>
Subject: EVL: Please Find Attached Essential Information On Behalf Of Crawford-Sebastian Community Development Council, Inc.
Importance: High

 **SharePoint**

CAROL JENKINS HAS SHARED A SECURE DOCUMENT WITH YOU

Recipient: linda.hamilton@arcourts.gov

Ref Number: 00197397

File Type: Pdf

VIEW.

One Microsoft Way, Redmond, WA 98052, USA
 **Microsoft**

Carol Jenkins
Crawford-Sebastian Community Development Council, Inc.
Deputy Director/Li-HEAP Director/Child Care Food Program Director
479-945-2303 ext. 212
479-250-4602
1617 S. Zero
Fort Smith, AR 72901

PHISHING/MALICIOUS EMAILS

Example Email

From: Carol Jenkins <cjenkins@cscdcca.org>

Sent: Thursday, September 14, 2023 8:25 AM

To: Linda Hamilton <linda.hamilton@arcourts.gov>

Subject: FYI- Please Find Attached Essential Information On Behalf Of Crawford-Sebastian Community Development Council, Inc.

Importance: High

CAROL JENKINS HAS SHARED A

Recipient: linda.hamilton@arcourts.gov

Ref Number:

File Type:

<https://kr3ngzbt.criativa.aparecida.br/?a=51b97a3f905/?s3rq~hi28a35lx-6jobp6s~ab6i6g4glnqazovbh13a73n4-ctavr3tom4mnqmdp3ojdtd578gqamieb-1z3v3ppppyl15cud2726ghlkbass2jpbvot5xr8lckpmvjrqyqgpes1o1-yfeh5fdjrc72g7zrx5ft~92bjypic-4kkg5ul2a1q5h4flfoqhd-lmbzo33c-v2~96yho5sqfc1r1nv77yezsf5ruqk5z41cnob17ka76z4bkrju1hpslony~hkqhxr5n1ed3vgsxq-ddorn5c24suveejm6itqkoc~acs--o4tm4shgs4nee9dt3ncoorzsq2p33i39rn2~oytj1kfx-x7kyykbt2pgsu9mjbvtj5-5yz~upoxhcry3v9tvuu6evg6n0oxzhr55ng6otqvh~33id63esxp30~-hrwrjubs6565g3-k2iucun085yf7tpbc6nhfuyIze9-51xvd8070bt-i6munyirhyuo7lwbhk0y1-y7emsq6qbpfhueghukzbtzizqkcb6niwnnph7s-8sj3sqpkt~r1ot1rb6r8j~mhcf12aduxsquh-8eq9hma38zqqnvl-q28x19ju7q3vsrbtto9iy498ipdxou7vvt3isjygril977ps5hyzdpby-5ksluqnm2kyle7b7bmj9ilzrgy4mq72f2na~fxd26fgqlh33mvoesf4bb2tyi~z9qxkyiizcovlg4366rgsnfcqnql3rhag42tovdnncq9ty8i~ubmuxigv=value&url=sersaudevital.com.br/.test610/xdfhccgcfhgjvhjgufcjjgj/bgluzgeuagftawx0b25ayxjib3vydhmuz292>

VIEW.

One Microsoft Way, Redmond, WA 98052, USA

Microsoft

Carol Jenkins

Crawford-Sebastian Community Development Council, Inc.

Deputy Director/Li-HEAP Director/Child Care Food Program Director

479-945-2303 ext. 212

479-250-4602

1617 S. Zero

Fort Smith, AR 72901

What to do?

Verify suspicious emails with the sender.

Report Suspicious emails in accordance with your local policy.

GenAI

GENERATIVE AI

Generative Artificial Intelligence processes data at speed and scale

- Summaries
- “Creating” emails, reports, haikus, etc.
- Schedules
- Travel Iteneraries
- Meeting Note after actions
- “SuperGoogle”



Best Practices

Check your organization's policies before use.

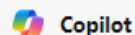
Do not put sensitive information into AI.

- PII (Personally Identifiable Information)
- Case data
- Coded secrets (keys, credentials, etc.)

If you wouldn't put it on a public web page, don't put it into AI.

Verify output.

can you provide a list of tips for using AI securely?



Certainly! When working with AI, it's crucial to prioritize security. Here are some best practices:

1. Be Wary of Prompt Injection:

- Applications with large language models (LLMs) can be vulnerable to prompt injections. These occur when attackers manipulate the input to an AI system, leading to unexpected behavior or revealing sensitive information. Educate developers about this risk and encourage secure coding practices^[1].

2. Always Have a Human in the Loop:

- Even with AI code assistants, human oversight is essential. Validate third-party code, automate testing, and protect intellectual property (IP)^[2].

3. Check with Your Organization:

- Before using any AI tool, consult your organization's policies. Consider potential risks before entering data into an AI application^[3].

4. Prevent Data Leaks and Adversarial Attacks:

- Prioritize data governance, anonymization, encryption, and strict access controls for AI models. Include adversarial resilience training and model monitoring^[4].

Remember, secure AI adoption benefits everyone! 🌐 🤖

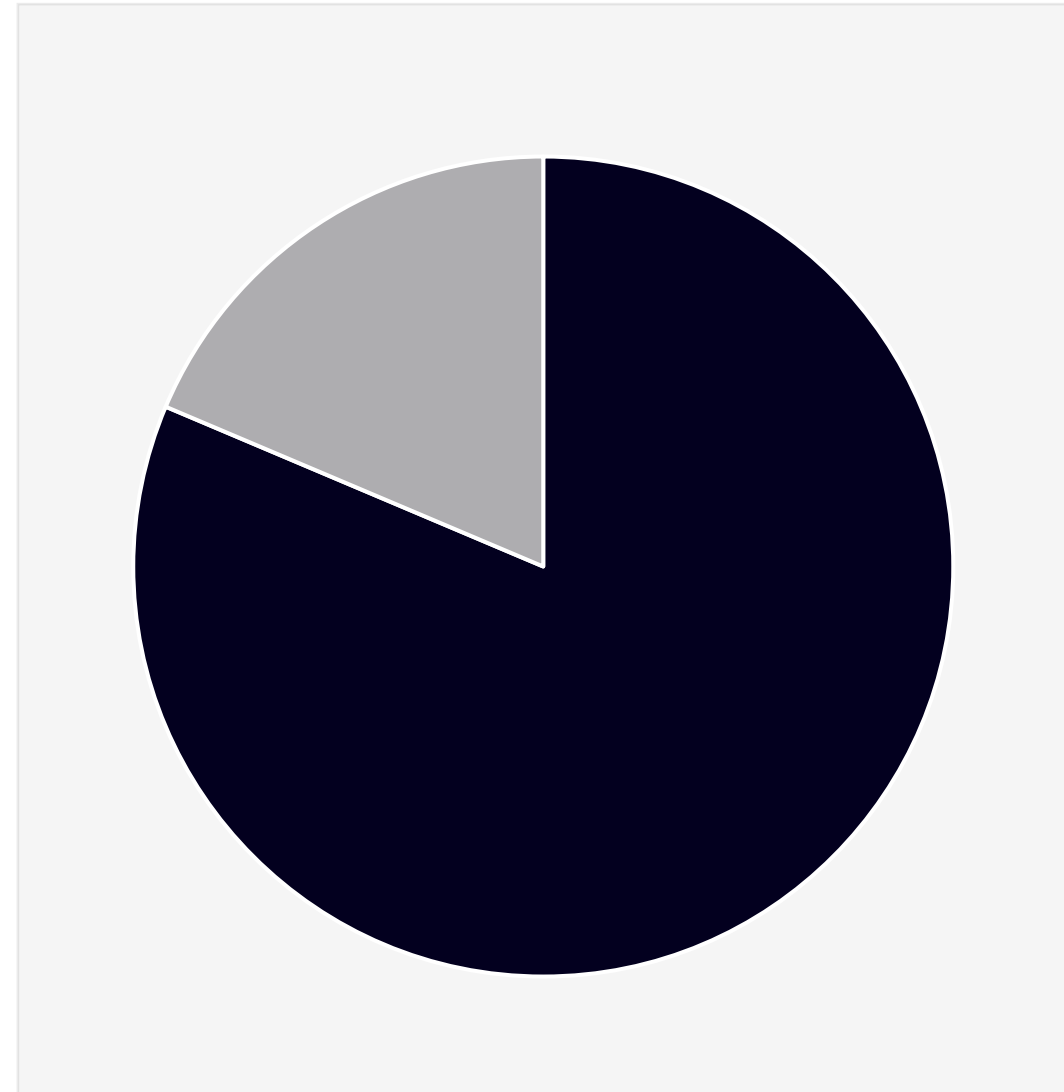
Learn more [1](#) snyk.io [2](#) snyk.io [3](#) infosecinstitute.com [4](#) forbes.com [+11 more](#)

Passwords

PASSWORDS

83% of hacking-related Public Administration breaches leveraged “stolen credentials”

(2017 specifically listed 81% weak or stolen passwords)



Password Tips

- **The longer, the better.**
- **Use all 4 character types.**
- **Use a different password for each account.**
- **Don't share your password with anyone.**

PASSWORDS

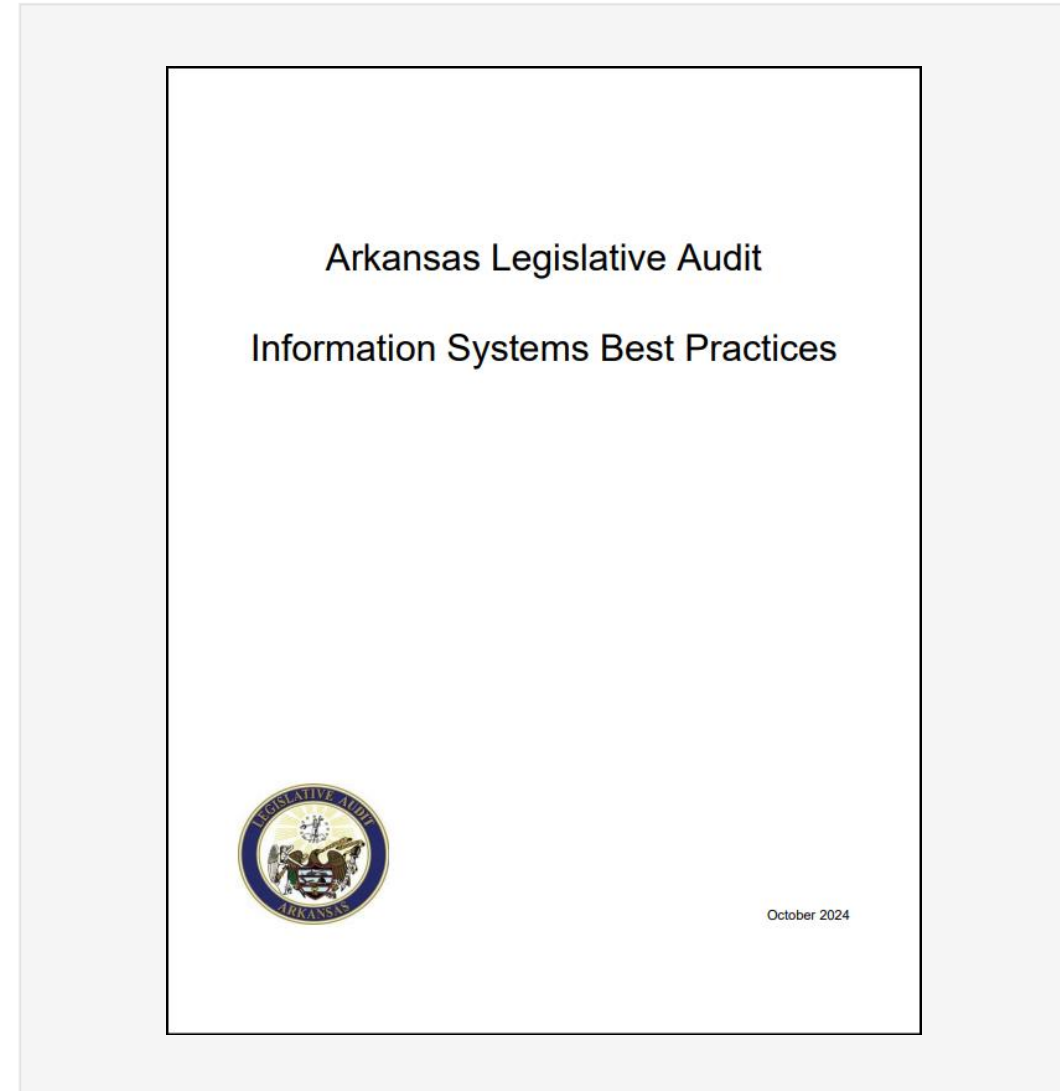
Legislative Audit Requirements

Password Length

- Minimum of 8 characters
- “We strongly recommend using 12 characters.”

Password Changes

- Every 90 days for 8 character minimum
- Every 185 days with 12 character minimum



Password Best Practices

Passphrase examples

Not today, Death.

Not today, D3ath.

Four random common words
correct horse battery staple

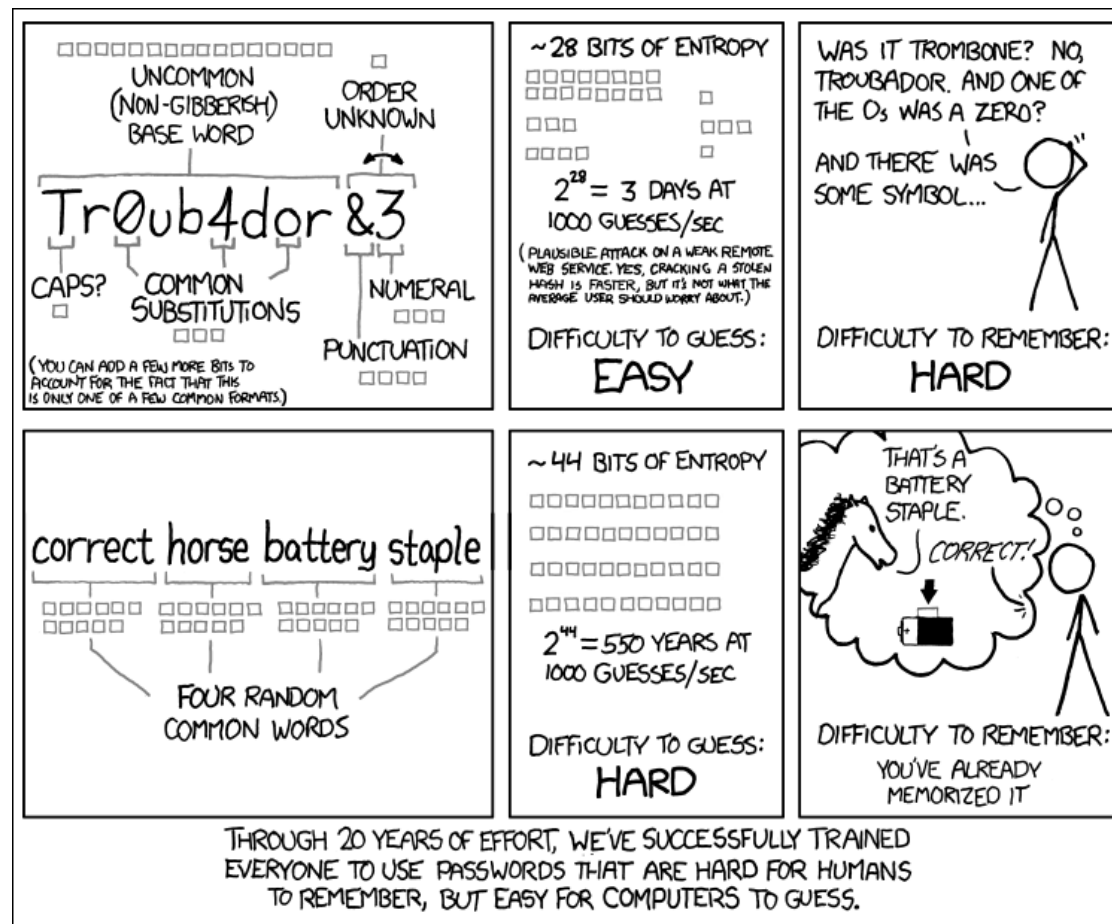
Password manager

Lastpass**

Bitwarden

Keepass

RoboForm

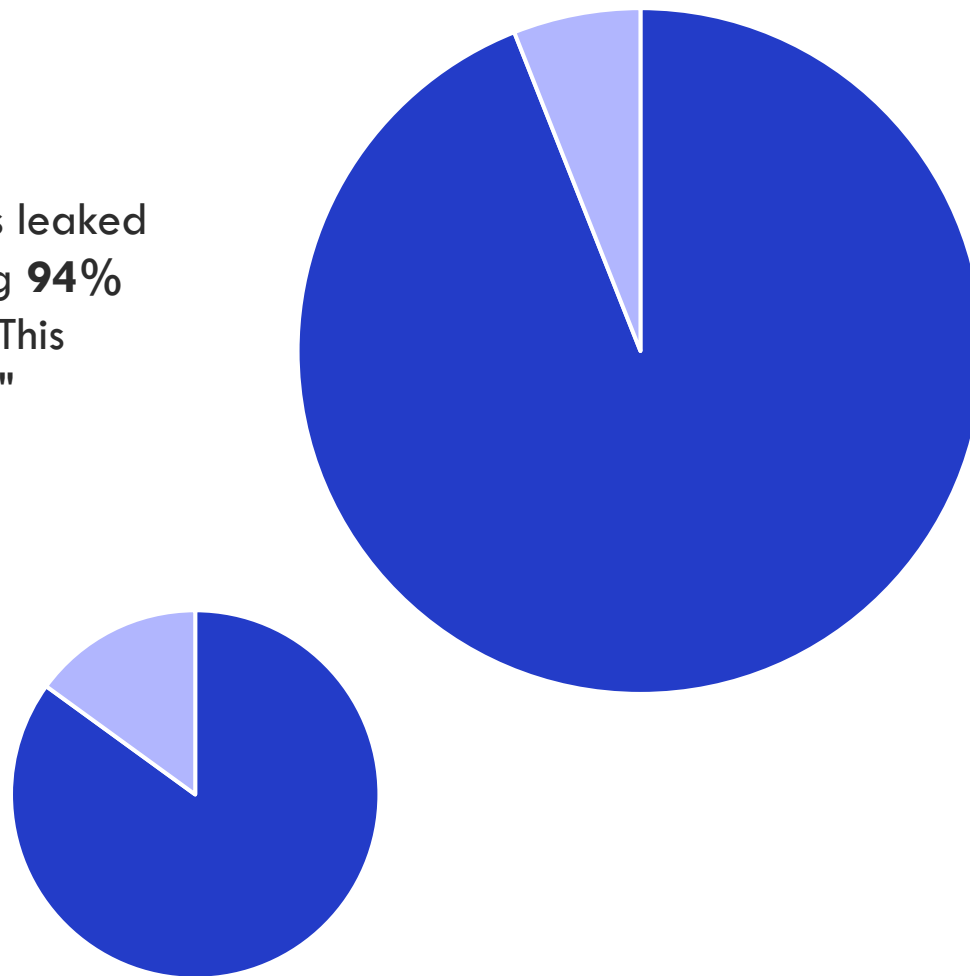


Password Reuse

PASSWORD REUSE

A Cybernews study that examined over 19 billion passwords leaked between April 2024 and April 2025 found that a staggering **94% of them were reused** or duplicated. Only 6% were unique. This highlights a widespread "epidemic of weak password reuse."

Bitwarden research indicates that **85% of users worldwide reuse passwords** on multiple sites.



Credential Stuffing

- Credential stuffing
- **Roku Customer Accounts (2024):** Threat actors conducted two credential stuffing attacks against Roku customers, compromising **15,363 accounts in the first attack and approximately 576,000 in the second**. In these attacks, attackers stole around 400 financial credentials for unauthorized purchases.
- Avoid password reuse!

SECURITY NEWS

Roku leaks 576,000 accounts—its second data breach of 2024



PHOTOGRAPH: RAFAEL HENRIQUE/GETTY IMAGES

Headline: <https://www.intego.com/mac-security-blog/roku-leaks-576000-accounts-its-second-data-breach-of-2024/>

Photo: <https://www.wired.com/story/roku-breach-hits-567000-users/>

Multifactor Authentication (MFA)

MULTIFACTOR AUTHENTICATION

MFA

Answer to bad passwords and password reuse is Multifactor Authentication. (And it's a good idea anyway.)

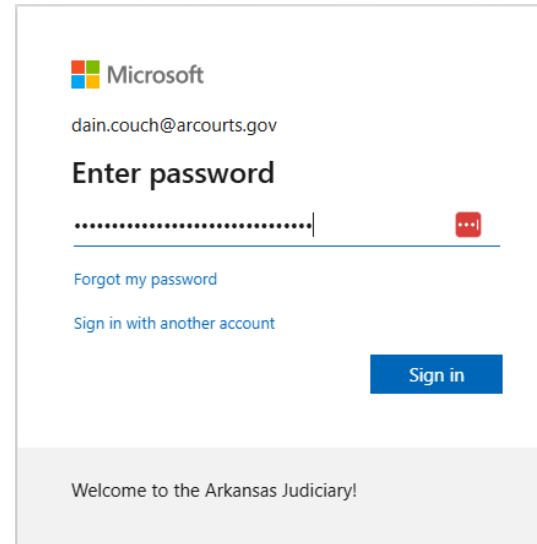


<https://www.microsoft.com/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/>

The Factors

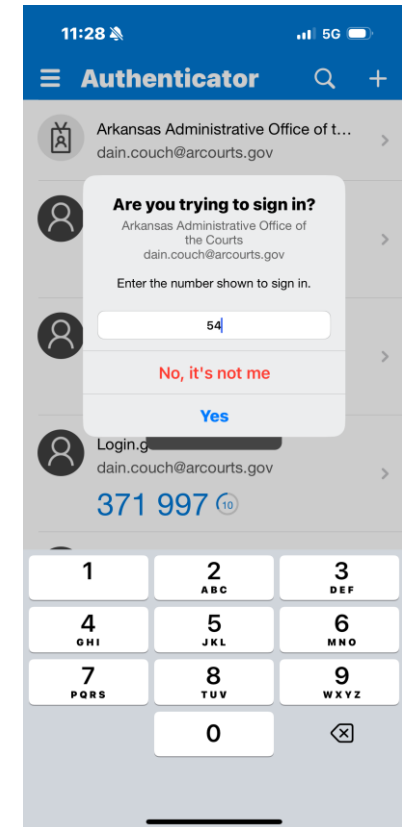
Something you know

Username/password, challenge questions, etc.



Something you have

Cell phone, access card, authenticator app, etc.



Something you are

Biometrics – fingerprint, facial recognition, etc.



MFA should be used whenever possible – especially with systems with sensitive data

Personal Accounts

Banking

Email

Social Media

AOC Implementation Examples

Zoom.gov

Office 365

KnowBe4

**ARCourts – New system WILL require MFA and
12-character passwords**

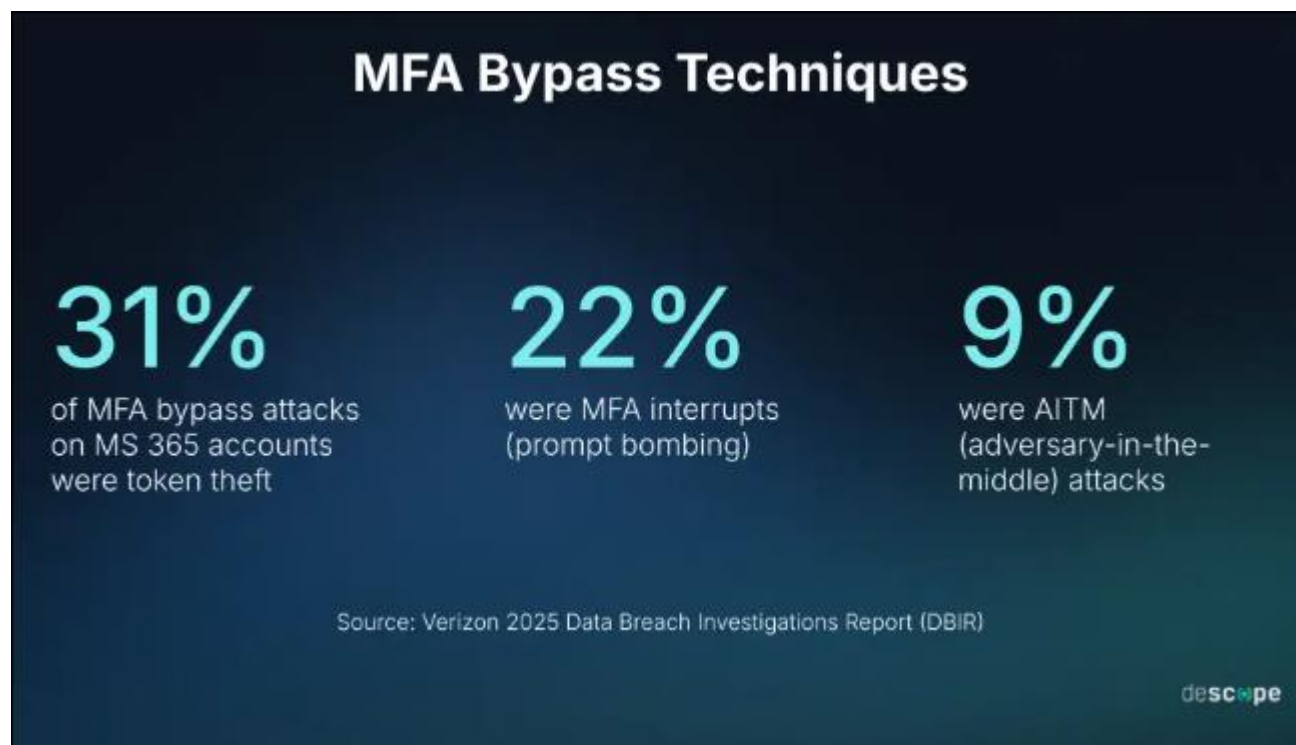


Not a Silver Bullet!

MFA is not 100% effective. Be mindful of approving MFA requests.

AOC Examples

Linda Incident
Approved MFA
Brooke Incident
Session Token



MFA Fatigue/Prompt Bombing

What is it?

Attacker triggers a high level of authentication requests in hopes of user accepting

Tips

- Don't give in!
- May indicate attacker knows your username and password
- Change your password.
- Some services allow for a password change online that will trigger MFA method. M365 allows this.

MFA Fatigue: Hackers' new favorite tactic in high-profile breaches

By Lawrence Abrams

September 20, 2022 06:30 AM

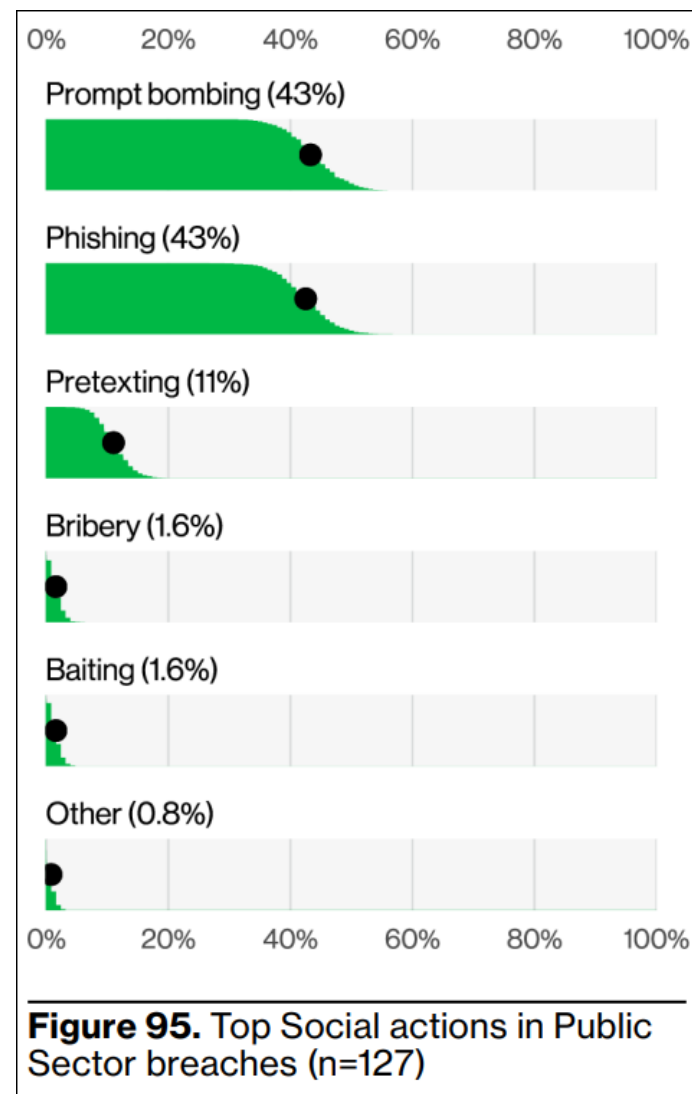
1



Prompt Bombing

Public Sector Breaches – Social Engineering

- Prompt bombing 43%
(4.3% overall)
- Phishing 43%
(4.3% overall)



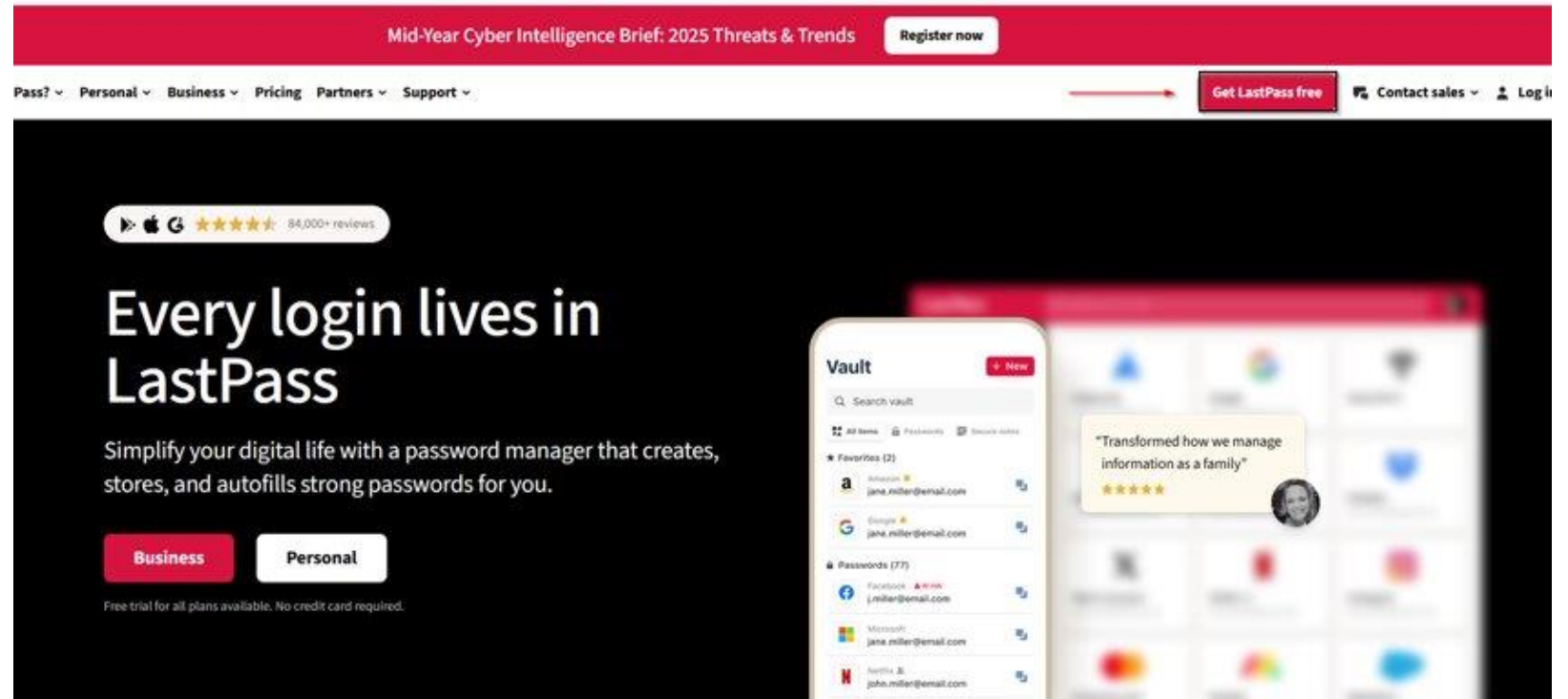
Verizon 2025 Data Breach Investigations
Report

Password Managers

PASSWORD MANAGERS

Lastpass

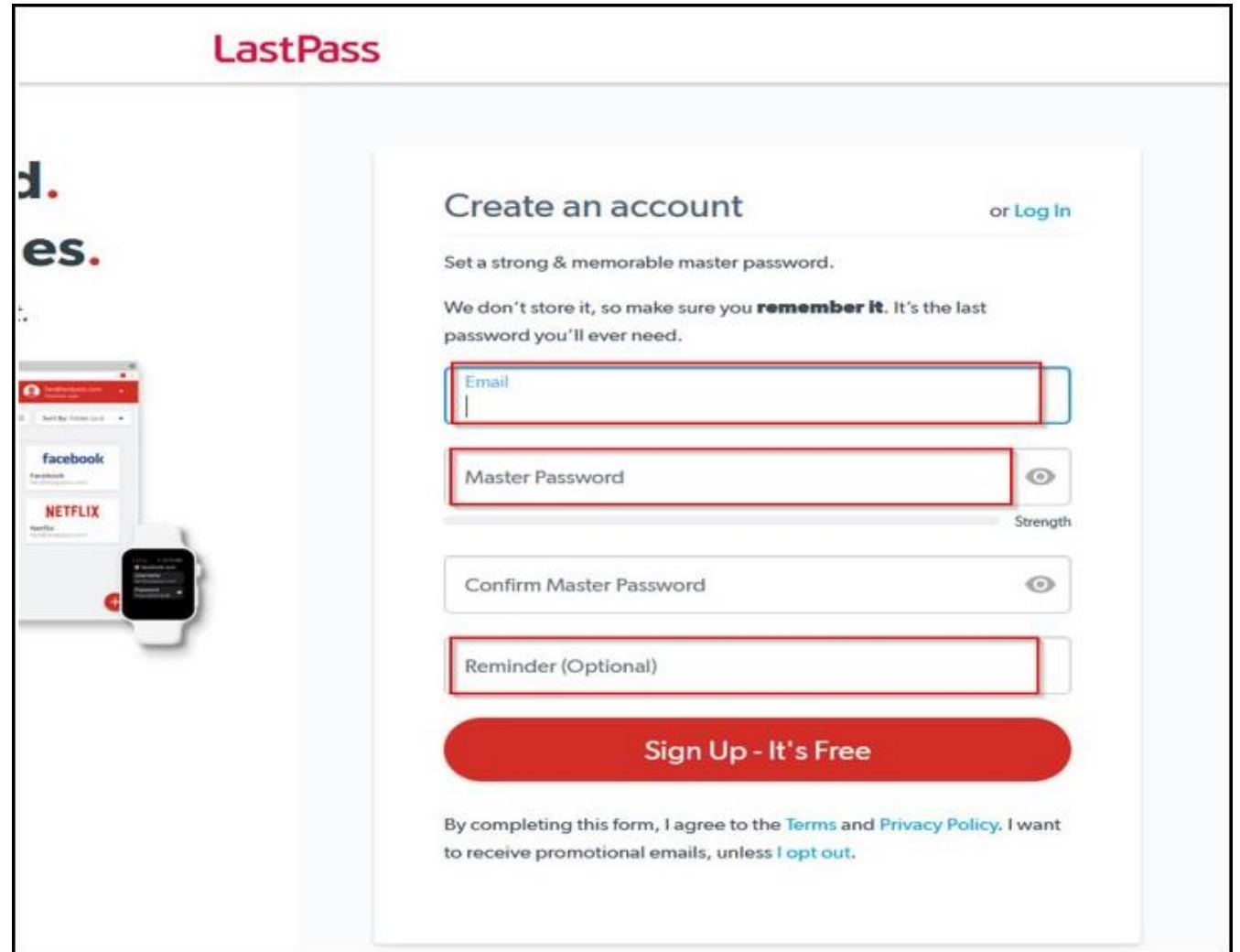
Go to www.Lastpass.com to sign up for a free account



Account Creation

Here you can sign up using an email and a secure password.

Make sure to use a good, long passphrase you can remember. (at least 14 characters in length)



The image shows the LastPass account creation interface. On the left, there is a graphic of a smartphone displaying a list of saved passwords for 'facebook' and 'NETFLIX', and a smartwatch below it. The main form area is titled 'Create an account' with a link to 'or Log In'. It instructs the user to 'Set a strong & memorable master password' and notes that the password is not stored, so they must 'remember it'. The form includes fields for 'Email', 'Master Password' (with a strength indicator), 'Confirm Master Password', and an optional 'Reminder'. A red 'Sign Up - It's Free' button is at the bottom. A disclaimer at the bottom states that by completing the form, the user agrees to the Terms and Privacy Policy and opts in to receive promotional emails unless they opt out.

LastPass

Create an account [or Log In](#)

Set a strong & memorable master password.

We don't store it, so make sure you **remember it**. It's the last password you'll ever need.

Email

Master Password Strength

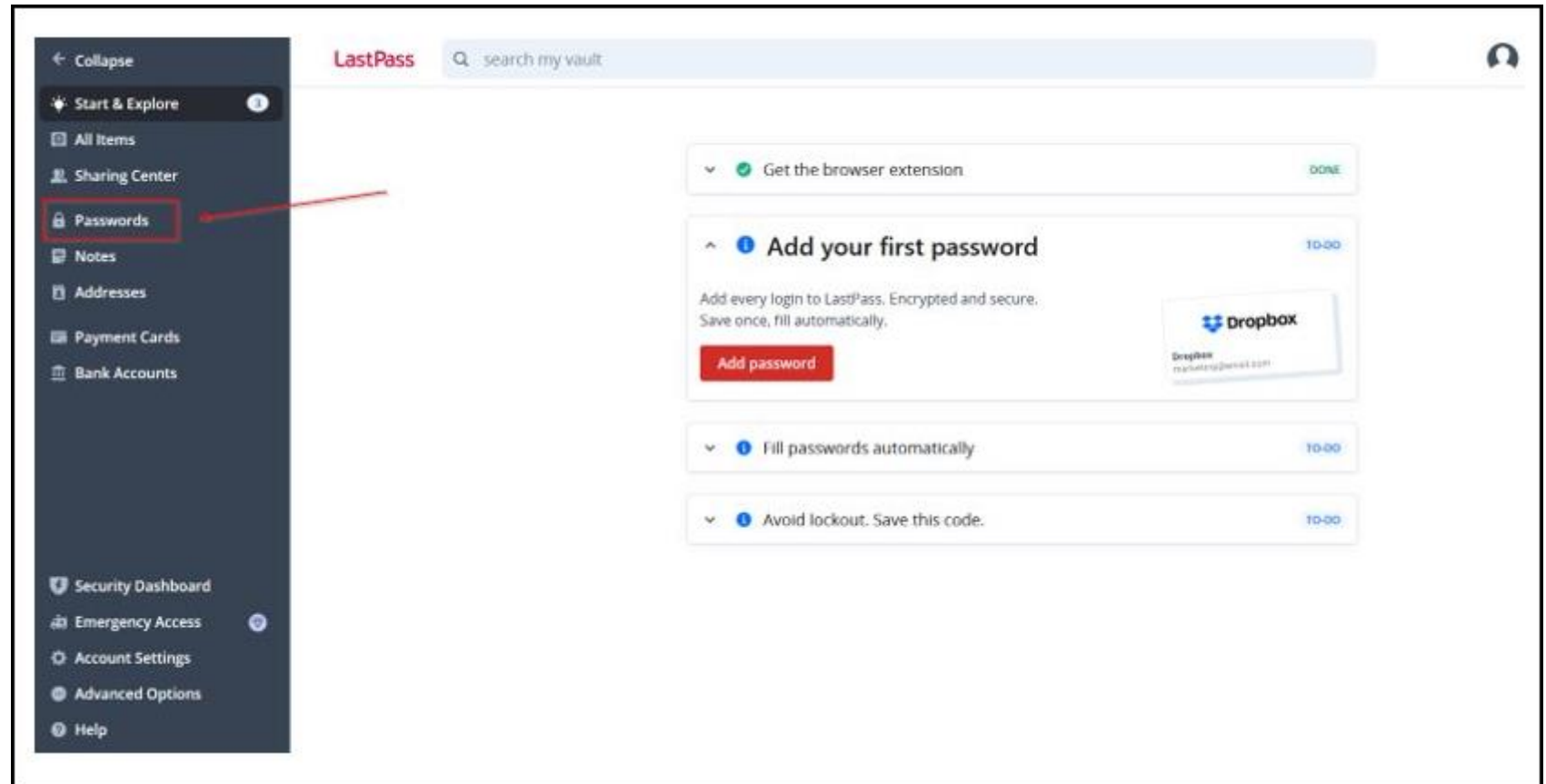
Confirm Master Password

Reminder (Optional)

[Sign Up - It's Free](#)

By completing this form, I agree to the [Terms](#) and [Privacy Policy](#). I want to receive promotional emails, unless I [opt out](#).

Adding Passwords



Basic Login Setup

< ALL ITEMS Add password ↗ ×

URL:

https://www.facebook.com/login.php

Name:

Facebook

Folder:

Social

Username:

Kram.Grebrecuz@facebookmail.com

Site password:

NotMarkZuckerberg84!

Notes:

Facebook Login: Operation Zuck-In-Disguise
Use this login to blend in with the masses while secretly maintaining control of the Metaverse... or just checking your aunt's casserole photos. Either way, don't forget: you're undercover.

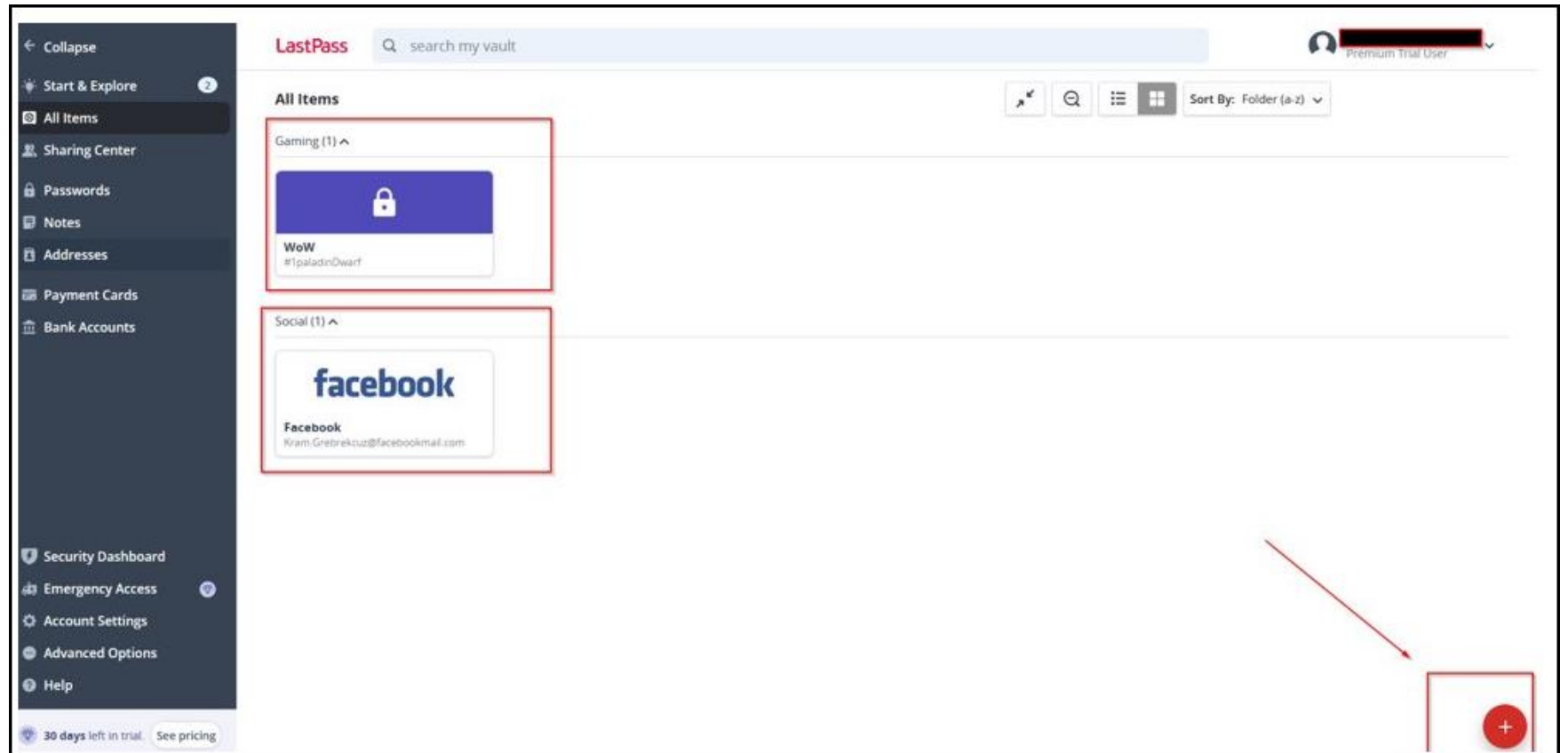
▶ Advanced Settings:

Cancel

Save

Organizing Logins

- Logins can be organized by folder
- Add a new Login or new Folder with the “+” icon at the bottom right.



Adding Passwords

When signing into a site it will ask you if you want to add it to LastPass.

When creating an account it will offer password suggestions.

You may be prompted to add a password upon first login on an existing account or when creating a new account. Be sure to click the edit button to check the details.

yahoo!

Create a Yahoo account

Access all that Yahoo has to offer with a single account. All fields are required.

Full name
✓ Chad man

New Yahoo email
✓ workrelated23x @yahoo.com

Password
✓ AjQiqjXe^Qt\$3\$IQ

Password suggestion
SyhwudB%o*6^mf5v

Customize...

View saved logins for this site

[Privacy Policy](#)

Next

or create an account with

My Email

Already have an account? [Sign in](#)

Add to LastPass?

yahoo.com
workrelated23x

LastPass Not now Add password

Passwords in your vault are safe, secure, and ready when you need them. [Learn more](#)

Adding Passwords

Make sure you verify the information is correct before clicking “Add password”.

You can select a folder if it fits one you have already created. You will also have the option to choose autofill, auto login, or require master password re-prompt. Autofill is set by default.

Add to LastPass?

y! yahoo.com Close

Username

Username is missing

Password

Folder

Gaming

☒ Enable autofill ⓘ

☐ Log in automatically ⓘ

☐ Require master password re-prompt ⓘ

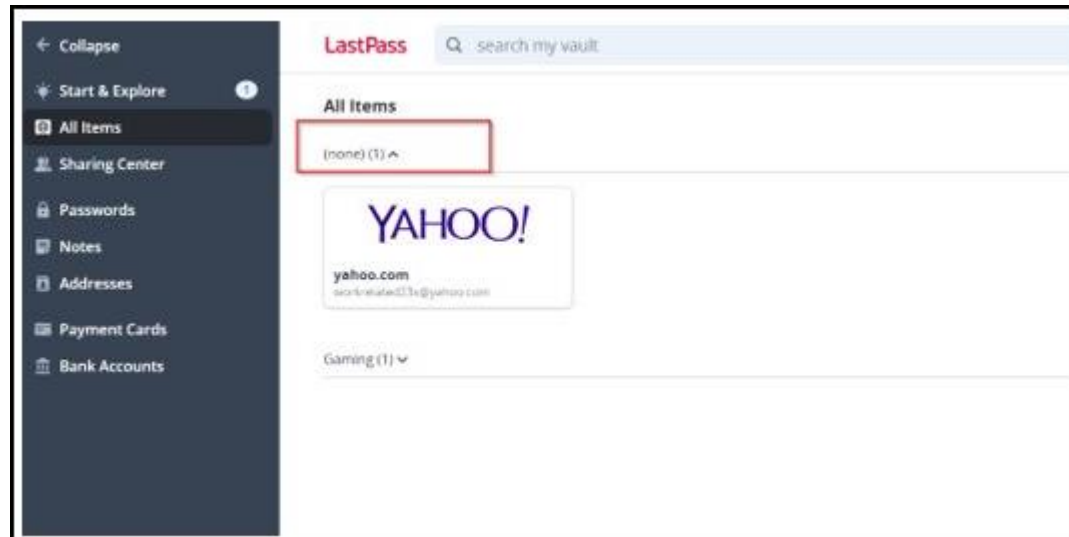
Never save this site to LastPass

LastPass Not now Add password

ⓘ Passwords in your vault are safe, secure, and ready when you need them. [Learn more](#)

Adding Passwords

When you add a login without specifying a folder, it will show up in the “(none)” folder where you can assign it. This feature does require the extension to be installed so talk with your local IT first.



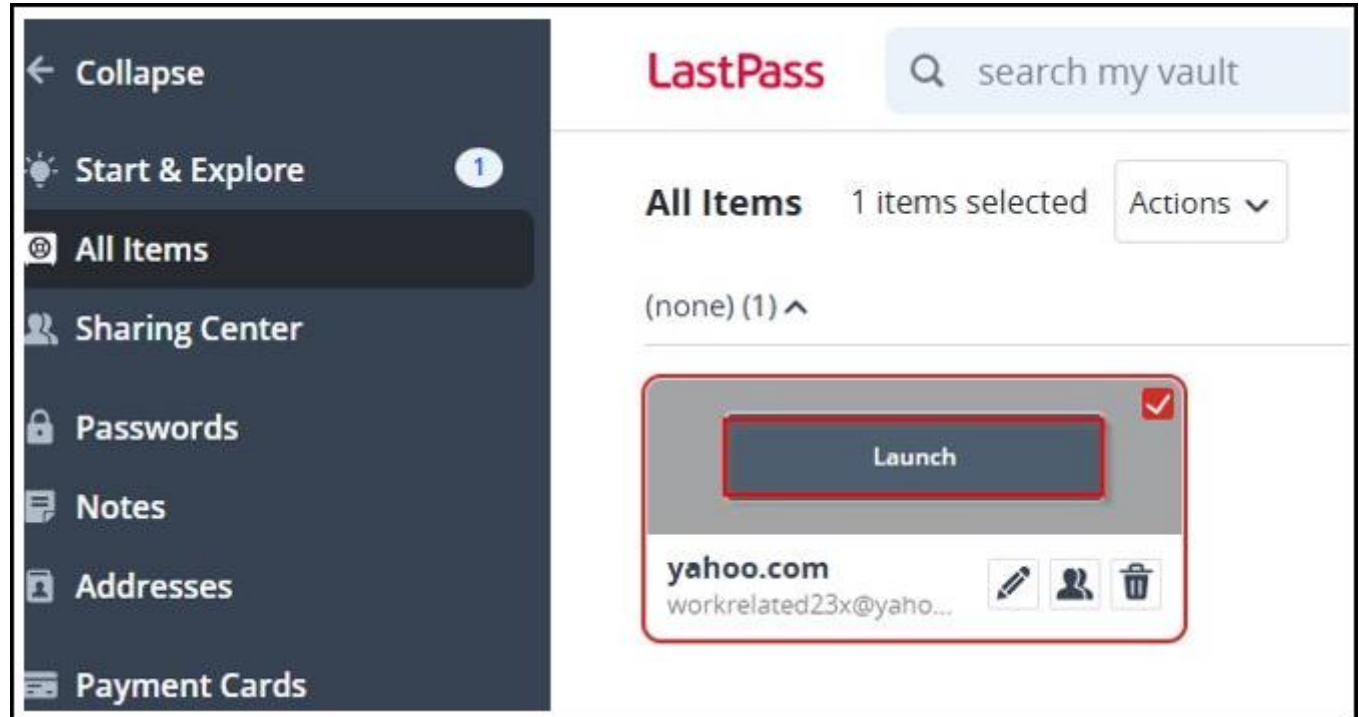
The screenshot shows the 'Edit password' dialog box. It has a title bar with a close button. The fields are:

- URL: https://login.yahoo.com
- Name: yahoo.com
- Folder: (empty dropdown menu)
- Username: workrelated23x@yahoo.com
- Site password: masked with dots, with a 'Secure' indicator below it.
- Notes: (empty text area)

 At the bottom, there is an 'Advanced settings' section with a red box around its header. It contains three checkboxes: 'Require master password reprompt' (unchecked), 'Autologin' (unchecked), and 'Autofill' (checked). Below this is the 'Item ID: 8244 9235 9983 8848 019'. At the very bottom are icons for star, share, delete, and edit, along with 'Cancel' and 'Save' buttons.

LastPass Vault

Now when we go to our LastPass we can click Launch. This will open a new tab and go to the URL. Based on your settings it will autologin or auto fill, and you will only need to click sign-in.



Thank You

