Cheatography

Social Media Account Security Cheat Sheet

by serracheats via cheatography.com/205691/cs/43895/

Social Media Safety Cheat Sheet

As always, please reach out to Security if you have any questions or concerns, or would like help configuring anything!

Strong Passwords

Use a combination of letters, numbers, and special characters.

Avoid using easily guessable information (birthdays, common words).

Change passwords if account shows suspicious activity.

Store passwords in a password manager. Use a unique password for each account.

Best Practices For Shared Accounts

Phishing Attempts!

Avoid clicking on suspicious links in messages or emails.

Verify the source before providing personal information.

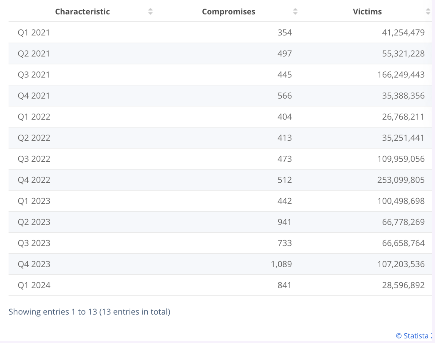
Look for signs of phishing: misspellings, urgent requests, unfamiliar senders.

Be skeptical of unsolicited messages and friend requests.

Keep an eye out for anything suspicious - ransomware attacks are on the rise!

Reminder: our Security Awareness training goes over phishing information, you can always review your training, or reach out to us with any questions!

Data Violation Incidents



Characteristic	Compromises	Victims
Q1 2021	354	41,254,479
Q2 2021	497	55,321,228
Q3 2021	445	166,249,443
Q4 2021	566	35,388,356
Q1 2022	404	26,768,211
Q2 2022	413	35,251,441
Q3 2022	473	109,959,056
Q4 2022	512	253,099,805
Q1 2023	442	100,498,698
Q2 2023	941	66,778,269
Q3 2023	733	66,658,764
Q4 2023	1,089	107,203,536
Q1 2024	841	28,596,892

Showing entries 1 to 13 (13 entries in total)

© Statista

This chart shows the number of data violation incidents and individuals impacted in the United States from 1st quarter 2021 to1st quarter 2024

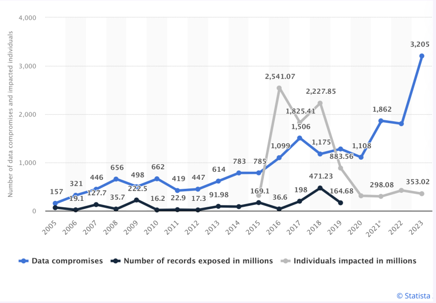
Incidents are quickly on the rise.

App Security

Only use trusted apps and websites to access your accounts.

Review permissions requested by third-party apps and integrations.

Data Compromise Counts



© Statista

Annual number of data compromises and individuals impacted in the United States from 2005 to 2023

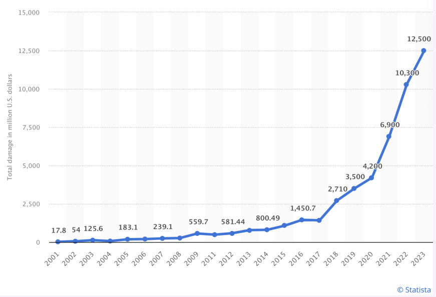
Multifactor Authentication (MFA)

Enable MFA on all accounts. The social media account itself, AND the email account associated with it.

Use your yubikeys on your accounts! (If they are compatible). If they are incompatible, use an authentication app (e.g., Google Authenticator).

Try to avoid SMS for the second factor, but it's better than nothing if it's all that's available.

Cost of Cybercrime



© Statista

Annual amount of monetary damage caused by reported cybercrime in the United States from 2001 to 2023 (in millions).

Compromised accounts cost a fair amount in both time and money, in addition to the

Use a centralized system to manage all corporate service accounts if possible.

Implement role-based access controls to restrict access to sensitive information and account control.

Use strong, unique passwords for each account. Use 1Password to securely share and store passwords. Avoid sharing passwords through insecure channels such as email or chat - this should ONLY happen through 1Password.

Create individual accounts for each user rather than sharing a single account.

Assign appropriate permissions based on user roles and responsibilities. Implement the principle of least privilege, granting users only the access necessary for their roles. Regularly review and update access permissions as roles and responsibilities change.

Enable MFA for all corporate accounts to add an extra layer of security. This should be set up in 1Password wherever possible. If not, document in the notes for an account how the MFA is set up!

Regularly review account activity logs to detect any unauthorized access.

Define and document clear policies for account access and usage.

Set up and maintain account recovery options for all corporate accounts. Ensure recovery information is up to date and accessible to authorized personnel.

Immediately deactivate accounts or revoke access for employees who leave the company or change roles.

Regularly review and clean up inactive or unnecessary accounts.

Revoke access for apps and integrations you no longer use.

Device Security

Keep your devices' operating systems and apps updated. Your laptops will do this through jamf settings, but your mobile devices will need to be monitored by you.

Lock your devices with passwords and biometric authentication. These are strongly preferred over PINs, and swipe lock should be avoided entirely.

Privacy Check Up

Regularly review and update privacy settings. Be sure to check account activity regularly for any suspicious behavior.

Limit who can see your posts and personal information.

Be cautious about sharing location data.

Review login attempts and account history.

Set up alerts for suspicious activity.

Don't hesitate to report and block malicious accounts/behavior.

personal stress of having to attempt recovery.