

SRHD IT Program



Ransomware,
Malware



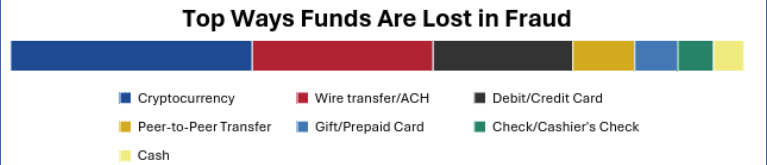
Phishing



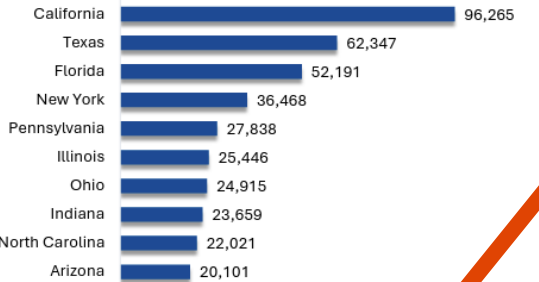
Data Breach

TOP REPORTED TRANSACTION TYPES¹⁵

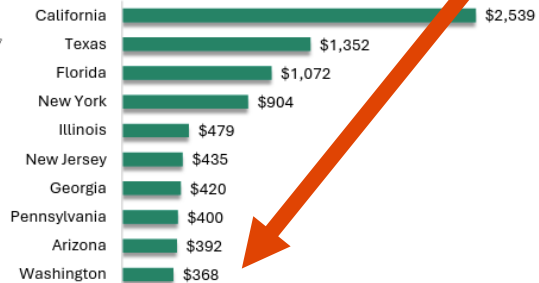
Transaction information provided in IC3 complaints helps FBI understand how victims are losing funds to fraud and assists the Recovery Asset Team Financial Fraud Kill Chain process when complaints are filed as quickly as possible. This chart identifies the top ways complainants reported financial loss in fraud.



**TOP 10 STATES
BY NUMBER
OF
COMPLAINTS**¹⁶



**TOP 10 STATES
BY LOSS (IN MILLIONS)**¹⁷



#10

+

- Time
- Energy
- Money

2024 CRIME TYPES *continued*

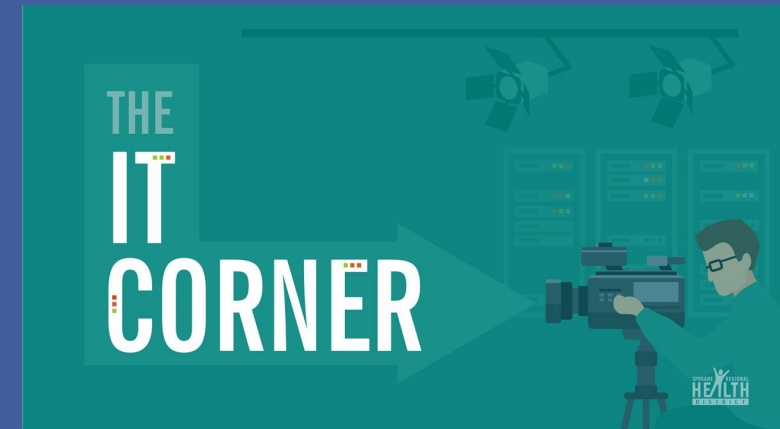
BY COMPLAINT LOSS			
Crime Type	Loss	Crime Type	Loss
Investment	\$6,570,639,864	Extortion	\$143,185,736
Business Email Compromise	\$2,770,151,146	Lottery/Sweepstakes/Inheritance	\$102,212,250
Tech Support	\$1,464,755,976	Advanced Fee	\$102,074,512
Personal Data Breach	\$1,453,296,303	Phishing/Spoofing	\$70,013,036
Non-Payment/Non-Delivery	\$785,436,888	SIM Swap	\$25,983,946
Confidence/Romance	\$672,009,052	Overpayment	\$21,452,521
Government Impersonation	\$405,624,084	Ransomware *	\$12,473,156
Data Breach	\$364,855,818	Harassment/Stalking	\$10,611,223
Other	\$280,278,325	Botnet	\$8,860,202
Employment	\$264,223,271	IPR/Copyright and Counterfeit	\$8,715,512
Credit Card/Check Fraud	\$199,889,841	Threats of Violence	\$1,842,186
Identity Theft	\$174,354,745	Malware	\$1,365,945
Real Estate	\$173,586,820	Crimes Against Children	\$519,424

FBI Internet Crime Report
2024



Knowledge

drip⁷



Friendly reminder to complete your Drip7 training

IT Administration
Cc Whitney Schlosser Naci Seyhanli

Reply Reply all Forward
Mon 5/19/2025 11:01 AM

Retention: 6 Year Delete (6 years) Expires: Sun 5/18/2031 11:01 AM

Hello,

This is a reminder to complete your May Drip7 training. This training is required for all employees to help keep our systems and data secure. Please take a few minutes to complete it by visiting <https://srhd.drip7.com>.

If you have any questions or need assistance, feel free to reach out! Thanks for helping keep us safe.

Thank you,

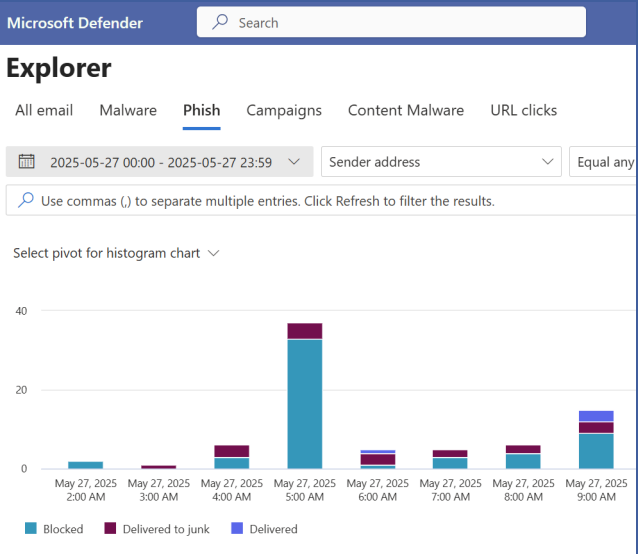


Information Technology
Spokane Regional Health District
Direct: 509.324.1513
srhd.org



Step 1: Protect the account

Multi-factor authentication,
Conditional access policies



Home > Spokane Regional Health District > Conditional Access

Conditional Access | Policies

Microsoft Entra ID

Overview

Policies

Insights and reporting

Diagnose and solve problems

Manage

Named locations

Custom controls (Preview)

Terms of use

VPN connectivity

Authentication contexts

Authentication strengths

Classic policies

Search

Add filter

12 out of 12 policies found

Policy name	Created by
Multifactor authentication and reauthentication for risky sign-ins	MICROSOFT
Multifactor authentication for admins accessing Microsoft Admin Portal	MICROSOFT
Multifactor authentication for per-user multifactor authentication users	MICROSOFT
Block Legacy Authentication	USER
Forti VPN domain joined devices only	USER
Location Block Non US	USER
MFA for Administrators	USER
Multifactor authentication for admins accessing Microsoft Admin Po...	USER



Step 2: Protect the email

Anti-phishing, Anti-spam,
Anti-malware

Step 3: Examine the content

Safe attachment
and Safe Link protections

Microsoft Defender

Policies & rules > Threat policies

Threat policies

Templated policies

Preset Security Policies	Easily configure protection by applying all policies at once using our recommended protection templates
Configuration analyzer	Identify issues in your current policy configuration to improve your security

Policies

Anti-phishing	Protect users from phishing attacks, and configure safety tips on suspicious messages.
Anti-spam	Protect your organization's email from spam, including what actions to take if spam is detected
Anti-malware	Protect your organization's email from malware, including what actions to take and who to notify if malware is detected
Safe Attachments	Protect your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Teams
Safe Links	Protect your users from opening and sharing malicious links in email messages and Office apps

Data Loss Prevention

Inspect the communication or file and control it.

Insider Risk Management

Look for indicators of a compromise and alert.

Audit: Who did what and when?



Purview

Endpoints (your computer and phone)

Is Windows updated? Is there a virus?

Identities (your account)

Is it you or does someone else have control?



Applications

What apps are people using?
How risky are they?



Defender

SRHD

Microsoft Defender

Search

Admin Seyhanli

Home

Incidents & alerts

Incidents

Alerts

Hunting

Actions & submissions

Threat intelligence

Learning hub

Trials

Partner catalog

Exposure management

Overview

Attack surface

Map

Attack paths

Exposure insights

Initiatives

Metrics

Recommendations

Events

Secure score

Data connectors

Microsoft Secure Score

OverviewRecommended actionsHistoryMetrics & trends

Microsoft Secure Score is a representation of your organization's security posture, and your opportunity to improve it.

Applied filters:

Your secure score

Secure Score: 74.75%

843.13/1128 points achieved

100%

80%

60%

02/2703/0503/1103/1703/2303/2904/0404/1004/1604/2204/2805/0405/1005/1605/26

Breakdown points by: Category

Identity92.41%

Data57.78%

Device73.56%

Apps74.39%

Actions to review

Regressed12

To address78

Planned0

Risk accepted1

Recently added0

Top recommended actions

Recommended action	Score impact	Status	Category
Block credential stealing from the Windows local security aut...	+0.8%	To address	Device
Disable 'Allow Basic authentication' for WinRM Service	+0.71%	To address	Device
Enable 'Local Security Authority (LSA) protection'	+0.71%	To address	Device
Disable the built-in Administrator account	+0.71%	To address	Device
Disable 'Allow Basic authentication' for WinRM Client	+0.71%	To address	Device
Set User Account Control (UAC) to automatically deny elevati...	+0.71%	To address	Device
Disable Solicited Remote Assistance	+0.71%	To address	Device
Enable scanning of removable drives during a full scan	+0.71%	To address	Device

Comparison

Your score74.75 / 100

Organizations of a similar size43.59 / 100

How could we evaluate our work?

SPokane

REGIONAL

HEALTH

DISTRICT

Microsoft Secure Score

Overview

Recommended actions

History

Microsoft Secure Score is a representation of your organization's security posture, and your opportunity to improve it.

Applied filters:

Your secure score

Include

Secure Score: 74.75%

843.13/1128 points achieved

What is a good Microsoft Secure Score?

Microsoft Secure Score is a measurement of an organisation's security posture, with a maximum score of 100. Secure Scores can vary depending on the size and complexity of the organisation, but a higher score indicates better adherence to security best practices.

Here are some guidelines for what might be considered a good score:

- **Above 80%:** This is generally considered excellent. Organisations with scores in this range have implemented most recommended security measures and are well-protected against common threats.
- **60%-80%:** This range is still good and indicates a solid security posture. There might be room for improvement, but **the organisation is likely taking security seriously.**
- **40%-60%:** This indicates a moderate level of security. While there are significant protections in place, there are also many opportunities for enhancement. Organisations in this range should prioritise improvements.
- **Below 40%:** This is typically seen as a low score and suggests that the organisation has considerable work to do in terms of security. Immediate action is recommended to address the most critical vulnerabilities.

Comparison

Your score

74.75 / 100

Organizations of a similar size

43.59 / 100

What's Next?

- More secure devices and
- Identities
- A more resilient network
- Continued outreach
- Refined policies and procedures



layers