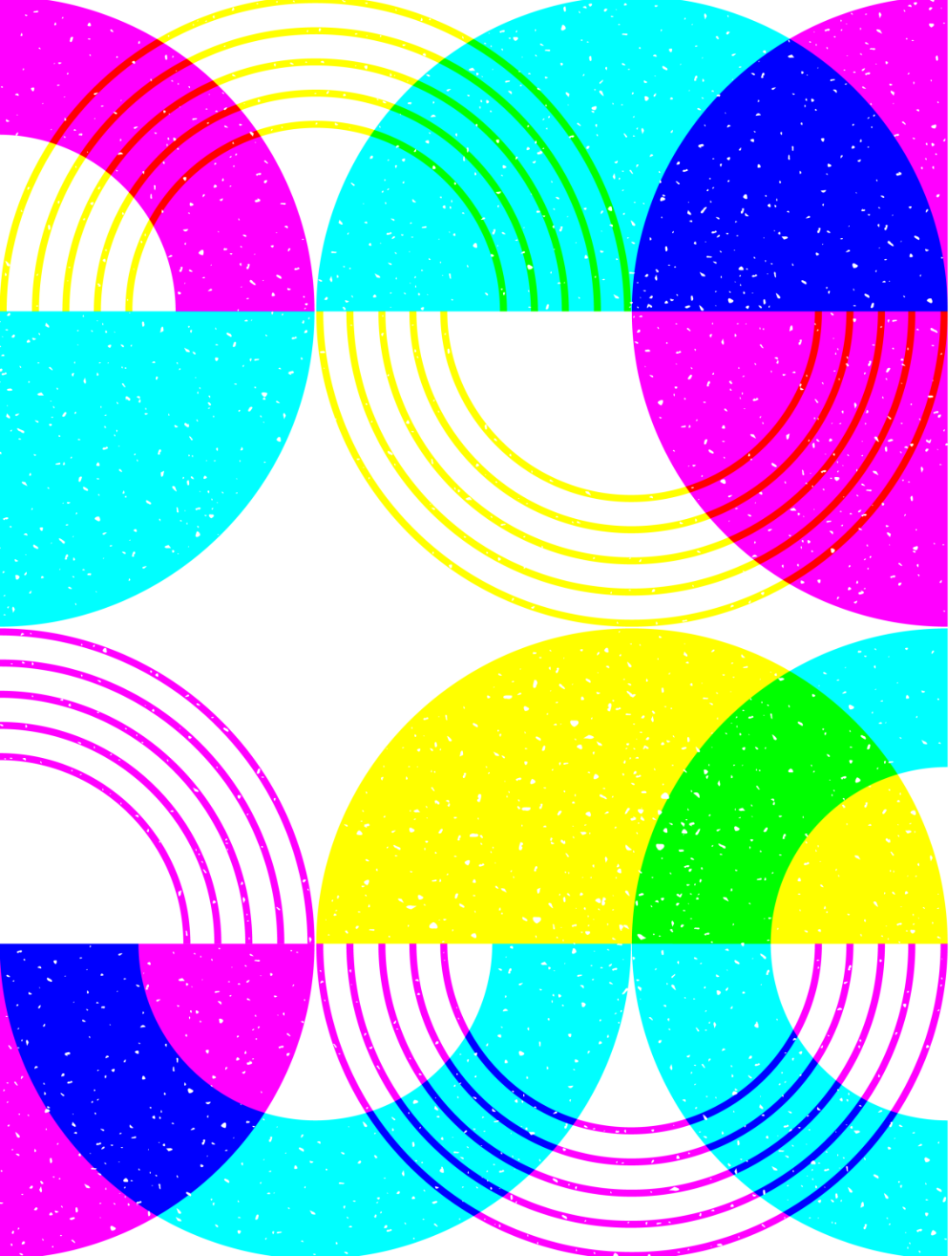


follow us on social!

#skyicon



SKYWARD®

iCON

Tracking the Trail - Investigating Unauthorized Access in Skyward

Mike Bianco – VP of Information Security

Investigating Unauthorized Access in Skyward

- What is Business Email Compromise (BEC)?
- How Can I Protect Our District?
- We've Been Compromised, What Do We Do Now?
- Forensic Investigations using Skyward Reports
- Improving Your Security Posture (homework handout)

What is Business Email Compromise (BEC)?

Business email compromise (BEC) is a type of cybercrime in which the bad actor uses **phishing emails** to trick employees into clicking on a malicious link that allows them to access their email accounts.

Using the email account, they use the **password reset** feature to gain access to Skyward.

Business Email Compromise often leads to **Financial Loss.** In 2023, the FBI received **21,489 BEC complaints**, with estimated **losses** of over **$2.9 billion**.



BEC: Payroll Fraud Example

Bad actors will:

Gain control of one or several email accounts within your district.

They often hide legitimate emails from the user(s).

They watch your email undetected, sometimes for months.



Shhh, Be vewy vewy quiet…..

Fraud Example 1

Bad Actors Masquerade as the victim(s)

- Bad Actors will request ACH change(s) to new bank account(s).
- Once they retrieve the funds, they close the account.
- The heist is complete before the victim asks about the missing paycheck.



Fraud Example 2

Bad Actors Masquerade as a Business Manager

- Bad Actors will make payroll or vendor ACH change(s) to new bank account(s).
- Once they retrieve the funds, they close the account.
- The heist is complete before the victim asks about the missing paycheck.



How Can I Protect Our District?

Implement Business Office Safeguards

- **Establish more that one communication channel to verify significant transactions**
- **Remain vigilant of sudden changes in business practices**
- **Raise awareness for individuals responsible for handling money**
- **Understand red flags, such as:**
  - **Online Only banks such as GreenDot**
  - **Multiple employee ACH changes, sometimes using the same account numbers.**

What IT can do to Protect Your District



Invest in "Most Impactful" Skyward Security Measures

- **Implement Multi-factor authentication**
- **Start a Security Awareness Training Program**
- **Implement IP Address Security Restrictions**

Other Security Considerations

- **Implement Advanced Endpoint Protection (EDR/XDR)**
- **Backup often, INCLUDING air-gapped backups**
- **Consider Cloud Hosting**

We've Been Compromised; What Do We Do Now?

Victims of BEC

- File with the FBI's Internet Crime Complaint Center (IC3) at www.IC3.gov.
- Contact Skyward
  - Using the Unauthorized User Access Guide:
    - Determine who was compromised
    - Change passwords
    - Determine what data was changed
- File a claim with your Cyber Insurance.
- Contact the Bank and Victims
- Perform Lessons Learned Review
- **Improve Security**

What Tools Are Available For Unauthorized User Access?

Skyward Forensic Tools (Reports & Logs)

- Login History
- User Tracking / Usage History
- Email History
- Vendor History
- ACH History
- and many others….



Prevent Further Damage

Confirmed Security Incident



Choices:

- Lock the entire system
- Lock Impacted Users
- Force password changes
- Enact your Incident Response Plan

Identify the “WHO”

Determine Which Accounts are Compromised

Login History - Find Unauthorized Logins

- Unknown IP Address(es)
- Unusual Browser, OS versions
- Unusual Login Times
- If you know what was changed, backtrack to those that have access to make that change.



Goal: Determine Bad Actor IP Address(es) or other Indicators of compromise (IoC) such as browser, browser version, OS version, Cookie, etc.

Identify the “HOW”

Determine How the Bad Actors Compromised the Accounts

Email History – Search for Security Alerts

- New Login Device
- Password Change
- ACH Change



Identify the “WHAT”

Determine WHAT the Bad Actors Changed

- User Tracking / Usage History
  - Report based on User, IP, and Date ranges
- Vendor History
- ACH History
- and many others….

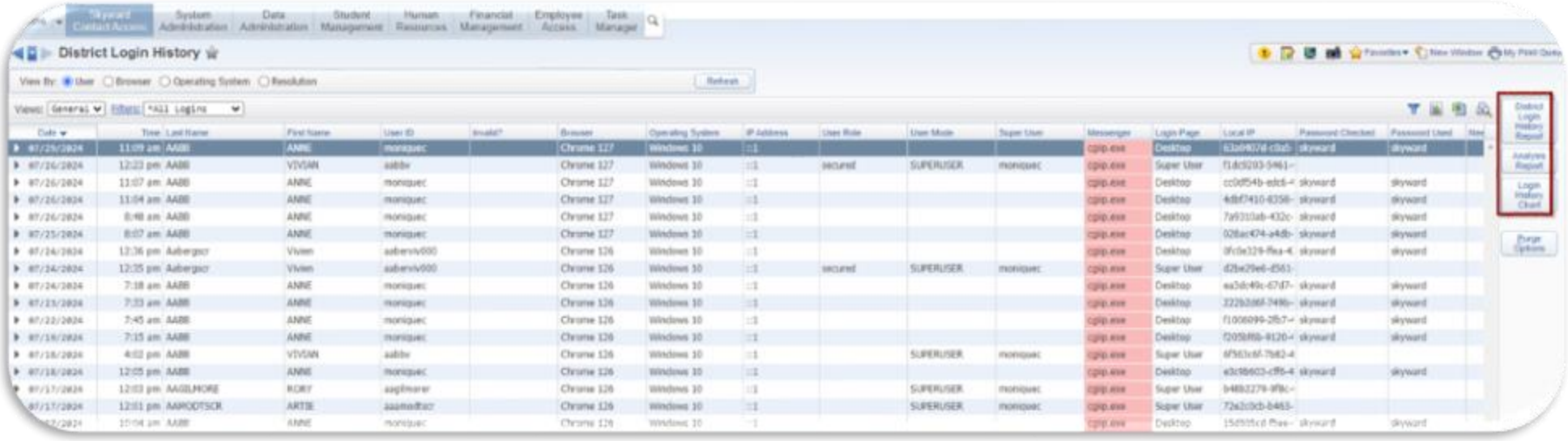


District Login History Searches

- Menu Path: Web Product Setup > Skyward Contact Access > District Login History.
- This area displays all users that have signed into the database allowing you view the date, time, browser, operating system, IP address, and their role and export to Excel.
- Create Filters to narrow your search, Export data to Excel

What to Look for:

1. Unusual Browser/IP Address/Operating System
2. Unusual Super User Activity
3. Unusual Dates/Times User Login

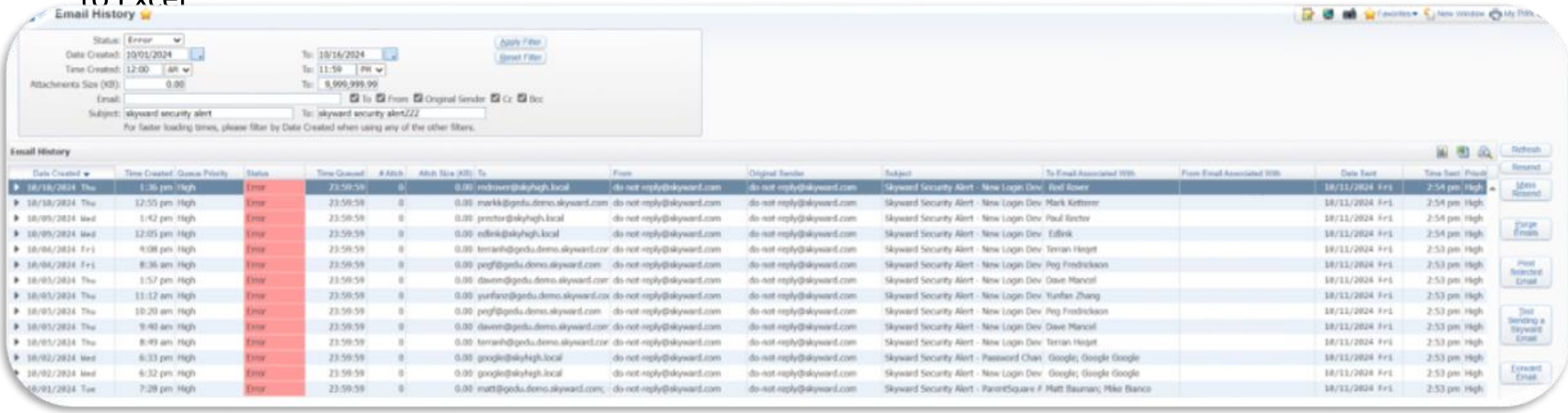


Email History Searches

- Menu Path: Web Product Setup > System Administration > Email History
- This area displays emails by the system, allowing you view the date, time, sender, recipient(s), subject, body, and more.
- User Filters and a Date Range to narrow your search, Export data to Excel

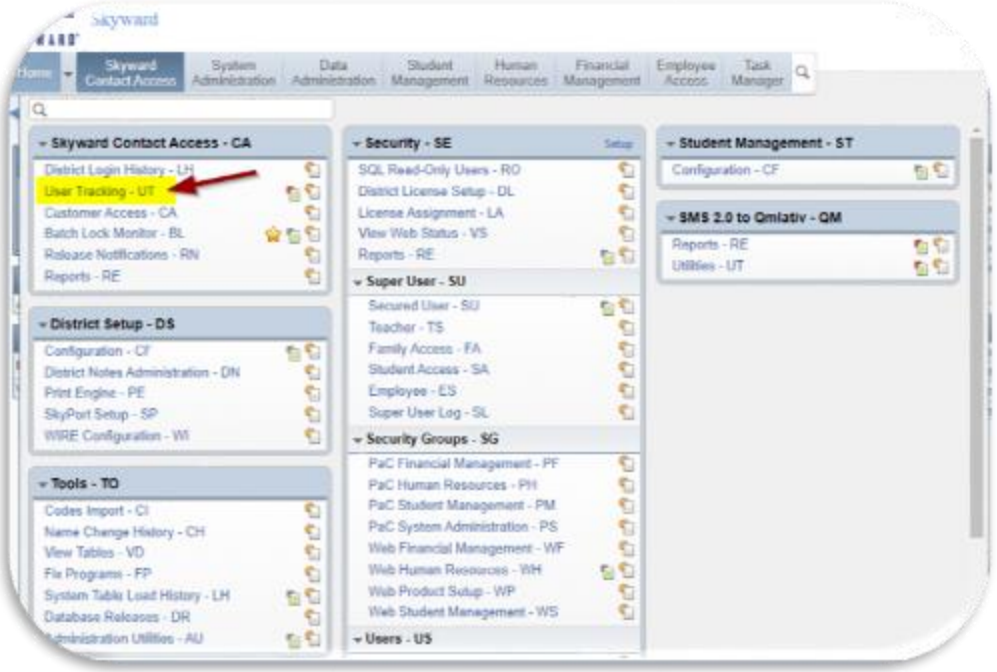
What to Look for:

1. Password Change
2. New Login Device
3. Direct Deposit Change



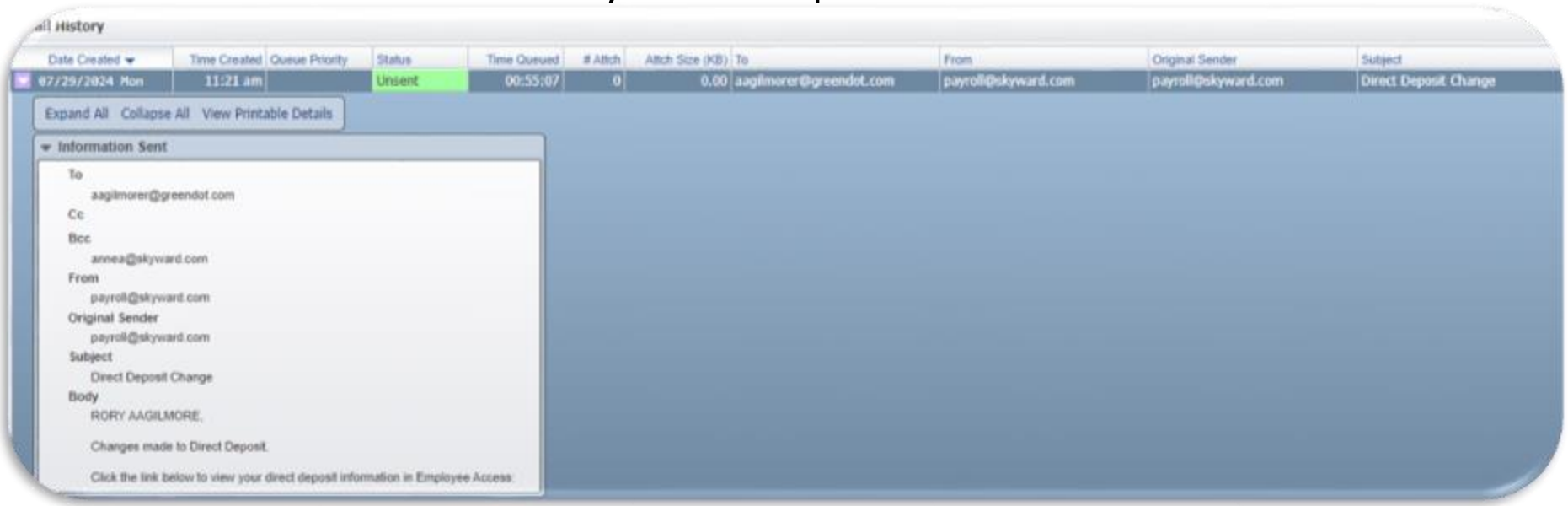
SMS 2.0 User Tracking Report

- Menu Path: Web Product Setup > Skyward Contact Access > User Tracking.
- Notes: This area allows staff to view and report users' activity within the software and tracks all menu paths that a user accesses; also shows "super user" logins (a user logging in under a different profile).
- Link to SkyDoc



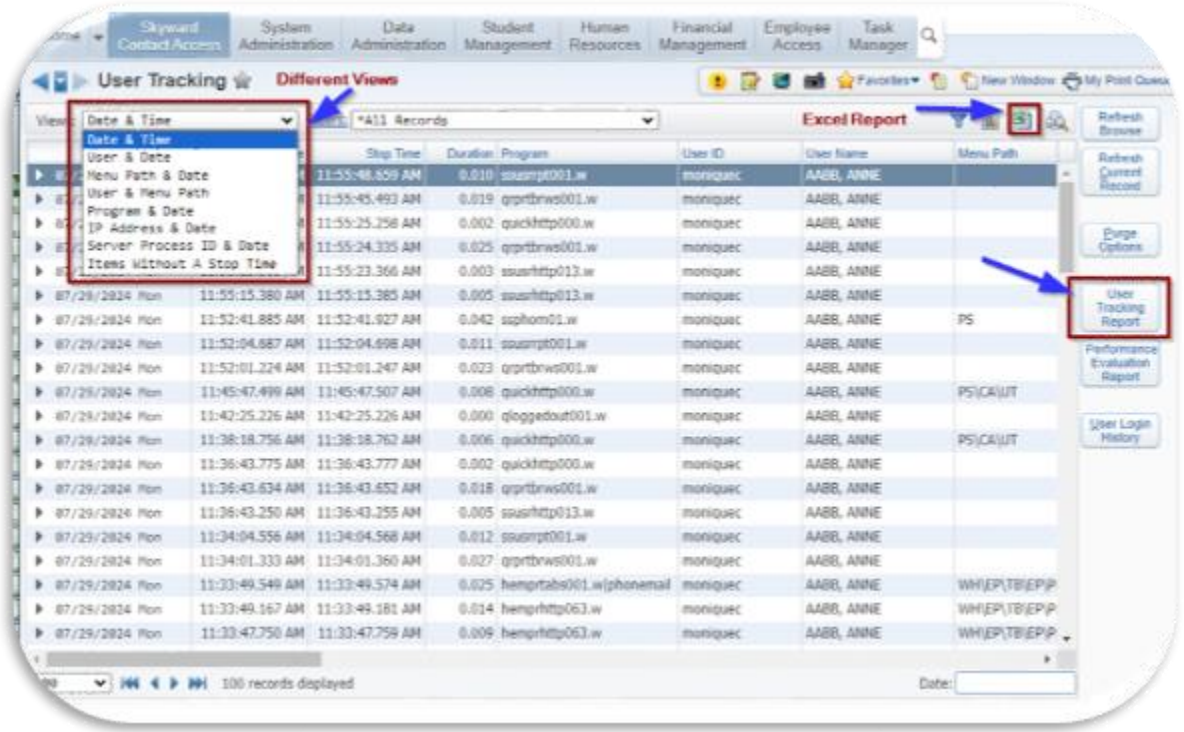
Example of Bad Actors with User Tracking

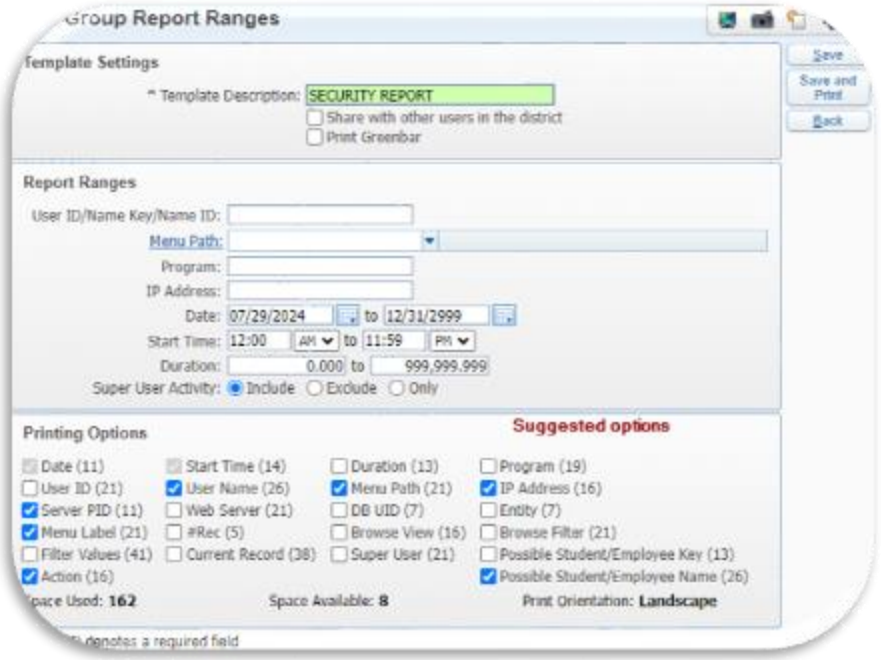
1. Bad Actor Hacks into Database through 3rd Party > Google Email Hack.
2. Change Email Address on an Employee Profile.
3. Change Direct Deposit Bank Info to Bad Bank.
4. Change the Email Address back to Original Email Address.
5. Now next Payroll will deposit into Bad Bank.



User Tracking Report

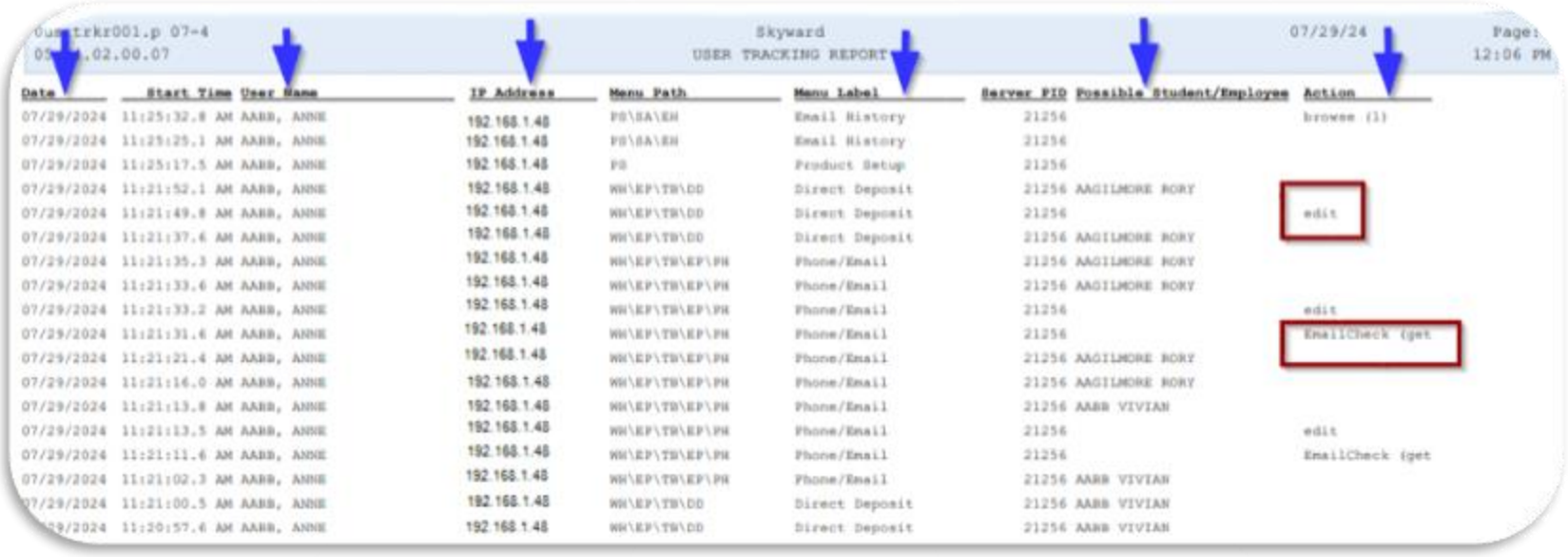
Can Export to Excel the Full Browse Screed to track activity OR run the User Report.





What to Look for:

1. View Email History Often to see any unusual activity.
2. View User Tracking to verify any unusual activity.
3. IP Addresses that are not familiar.
4. Unusual Actions.
5. Menu Paths that User doesn't visit per Job Type.



Skyward
USER TRACKING REPORT

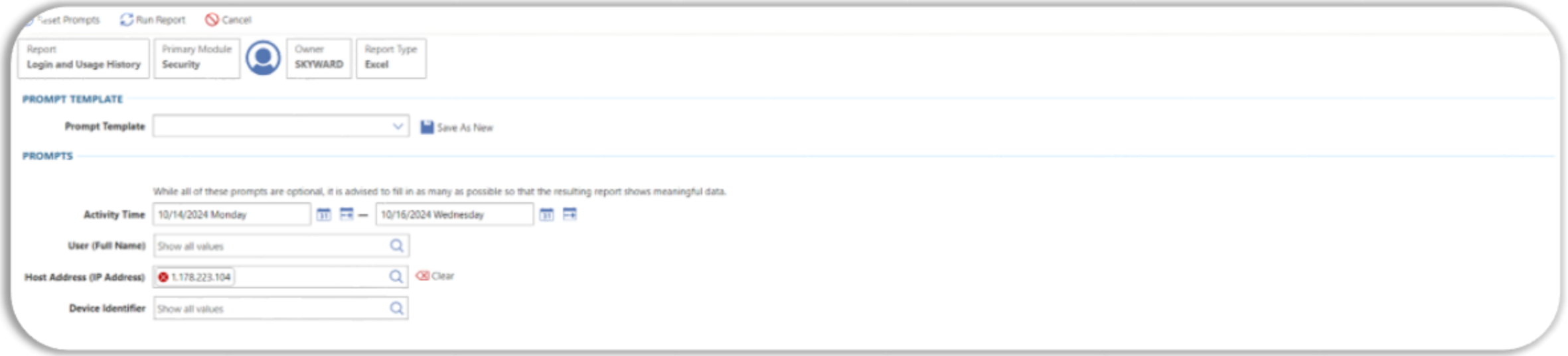
07/29/24 Page:
12:06 PM

Date	Start Time	User Name	IP Address	Menu Path	Menu Label	Server PID	Possible Student/Employee	Action
07/29/2024	11:25:32.8 AM	AABB, ANNE	192.168.1.48	PS\SA\EH	Email History	21256		browse (1)
07/29/2024	11:25:25.1 AM	AABB, ANNE	192.168.1.48	PS\SA\EH	Email History	21256		
07/29/2024	11:25:17.5 AM	AABB, ANNE	192.168.1.48	PS	Product Setup	21256		
07/29/2024	11:21:52.1 AM	AABB, ANNE	192.168.1.48	WH\EP\TH\DD	Direct Deposit	21256	AAGILMORE RORY	
07/29/2024	11:21:49.8 AM	AABB, ANNE	192.168.1.48	WH\EP\TH\DD	Direct Deposit	21256		edit
07/29/2024	11:21:37.6 AM	AABB, ANNE	192.168.1.48	WH\EP\TH\DD	Direct Deposit	21256	AAGILMORE RORY	
07/29/2024	11:21:35.3 AM	AABB, ANNE	192.168.1.48	WH\EP\TH\EP\PH	Phone/Email	21256	AAGILMORE RORY	
07/29/2024	11:21:33.6 AM	AABB, ANNE	192.168.1.48	WH\EP\TH\EP\PH	Phone/Email	21256	AAGILMORE RORY	
07/29/2024	11:21:33.2 AM	AABB, ANNE	192.168.1.48	WH\EP\TH\EP\PH	Phone/Email	21256		edit
07/29/2024	11:21:31.6 AM	AABB, ANNE	192.168.1.48	WH\EP\TH\EP\PH	Phone/Email	21256		EmailCheck (get
07/29/2024	11:21:21.4 AM	AABB, ANNE	192.168.1.48	WH\EP\TH\EP\PH	Phone/Email	21256	AAGILMORE RORY	
07/29/2024	11:21:16.0 AM	AABB, ANNE	192.168.1.48	WH\EP\TH\EP\PH	Phone/Email	21256	AAGILMORE RORY	
07/29/2024	11:21:13.8 AM	AABB, ANNE	192.168.1.48	WH\EP\TH\EP\PH	Phone/Email	21256	AABB VIVIAN	
07/29/2024	11:21:13.5 AM	AABB, ANNE	192.168.1.48	WH\EP\TH\EP\PH	Phone/Email	21256		edit
07/29/2024	11:21:11.6 AM	AABB, ANNE	192.168.1.48	WH\EP\TH\EP\PH	Phone/Email	21256		EmailCheck (get
07/29/2024	11:21:02.3 AM	AABB, ANNE	192.168.1.48	WH\EP\TH\EP\PH	Phone/Email	21256	AABB VIVIAN	
07/29/2024	11:21:00.5 AM	AABB, ANNE	192.168.1.48	WH\EP\TH\DD	Direct Deposit	21256	AABB VIVIAN	
07/29/2024	11:20:57.6 AM	AABB, ANNE	192.168.1.48	WH\EP\TH\DD	Direct Deposit	21256	AABB VIVIAN	

Qmlativ Security Report

Security module > **System Profile** feature > **Login and Usage History** report.

- Enter an activity time to narrow window of history.
- If known, Enter User(s), Host IP Address(es), or Device Identifier(s).
- Run Report > Download, Unzip, and \Review the report.
- Exports the Login and Usage history reports using a workflow



Qmlativ District Login History

Alternatively, you can review the District Login History screen

System module > **System Profile** feature > **General** tab group > **Login History** subtab

- Filter on Created time to narrow window of logins.
- Filter on Full Name or Username if you've identified users whose account has been compromised.
- For unsuccessful login attempts, filter on "Successful Login = False".
- Drop login data to Excel and remove duplicate Host Addresses to get a list of all the IP Addresses used to log in.
- IP address lookup tools can be found on a browser search to allow you to find the location of the login.

Qmlativ Usage History

Alternatively, you can review the Usage History screen.

System module > **System Profile** feature > **General** tab group > **Usage History.**

Usage History is kept for 31 days; this setting can be adjusted within the

System module > **System Configuration** setting > **General** tab group > **Configuration** subtab > **Days to store Usage History** field.


IMPROVE
SCHOOL
SECURITY

SMS 2.0: Security Tips for Your IT Staff

- **SMS 2.0 Multi-Factor Authentication**
  - Option 1: SMS 2.0 Native Multi-Factor Authentication
  - Option 2: Configure SSO using the SMS 2.0 SkySTS Server Launch Kit
- **Implement Security Group IP Restrictions**
  - SMS 2.0 Security Group IP Restrictions
- **Implement an Employee Security Awareness Training Program to raise awareness for individuals responsible for handling money.**
- **Skyward Security Best Practices→** https://www.skyward.com/blogs/skyward-insider/2024/september/skyward-security-best-practices

SMS 2.0: Unauthorized User Access Guides

The documentation links below will guide you through running reports to identify potential unauthorized access. We recommend that you focus on changes to PII or Financial information. The documents can also be found in Skydoc by searching for "Unauthorized Access" or the links below.

Student Guidelines - Unauthorized Access to Skyward Resources:
https://support.skyward.com/DeptDocs/Corporate/IT%20Services/Public%20Website/Technical%20Information/Administration/SMS%202.0%20Student%20-%20Skyward%20Guidelines%20-%20Unauthorized%20Access%20to%20Skyward%20Resources.pdf

Business Guidelines - Unauthorized Access to Skyward Resources:
https://support.skyward.com/DeptDocs/Corporate/IT%20Services/Public%20Website/Technical%20Information/Administration/SMS%202.0%20Business%20-%20Skyward%20Guidelines%20-%20Unauthorized%20Access%20to%20Skyward%20Resources.pdf

SMS 2.0 SECURITY TIPS FOR YOUR IT STAFF

VIEW THE PRESENTATION

View the presentation ***Cover Your Assets: Fraud Awareness and Prevention***:

SECURITY AWARENESS TRAINING

Implement an Employee Security Awareness Training Program to raise awareness for individuals responsible for handling money. Skyward Technology Solutions is a partner of KnowBe4, the leading Security Awareness Training program. For more information, visit:

SECURITY BEST PRACTICES

With today's sophisticated threats, it's essential to review your systems and take full advantage of built-in security features. To take a deep dive into security best practices for Skyward SMS 2.0 and Qmlativ, visit:

SECURITY TIPS

MULTI-FACTOR AUTHENTICATION

Use MFA to ensure only credentialed users are able to log in to your system:

SINGLE SIGN-ON

Save time while staying secure by configuring Single Sign-On for your applications:

SECURITY GROUP IP RESTRICTIONS

Limit access to secure resources with IP address range restrictions:

UNAUTHORIZED ACCESS

Use the guides below to learn how to run reports to identify potential unauthorized access to SMS 2.0 Student and Business resources.

SMS 2.0 STUDENT GUIDELINES

SMS 2.0 BUSINESS GUIDELINES

Qmlativ: Security Tips for Your IT Staff

- **Qmlativ Multi-Factor Authentication**
  - Option 1: Qmlativ Native Multi-Factor Authentication
    - (Hint: Open the Help Center before clicking the link or open the Help Center and search Multifactor Authentication in the Help Center.)
  - Option 2: Qmlativ SSO with an MFA-enabled Identity Provider
    - (Hint: Open the Help Center before clicking the link or open the Help Center and search SSO Launch Kit in the Help Center.)
- **Implement Security Group IP Restrictions**
  - Qmlativ Security Group IP Restrictions
    - (Hint: Open the Qmlativ Help Center before clicking the link or open the Help Center and search IP Address in the Help Center.)
- **Implement an Employee Security Awareness Training Program to raise awareness for individuals responsible for handling money.**
- **Skyward Security Best Practices→** https://www.skyward.com/blogs/skyward-insider/2024/september/skyward-security-best-practices

Qmlativ: Unauthorized User Access Guides

The documentation links below will guide you through running reports to identify potential unauthorized access. We recommend that you focus on changes to PII or Financial information. The documents can also be found in the Help Center by searching for "Unauthorized Access" or the links below.

Student Guidelines - Unauthorized Access to Skyward Resources:
https://support.skyward.com/DeptDocs/Corporate/IT%20Services/Public%20Website/Technical%20Information/Administration/Qmlativ%20Student%20-%20Skyward%20Guidelines%20-%20Unauthorized%20Access%20to%20Skyward%20Resources.pdf

Business Guidelines - Unauthorized Access to Skyward Resources:
https://support.skyward.com/DeptDocs/Corporate/IT%20Services/Public%20Website/Technical%20Information/Administration/Qmlativ%20Business%20-%20Skyward%20Guidelines%20-%20Unauthorized%20Access%20to%20Skyward%20Resouces.pdf

QMLATIV SECURITY TIPS FOR YOUR IT STAFF

VIEW THE PRESENTATION

View the presentation ***Cover Your Assets: Fraud Awareness and Prevention***:

SECURITY AWARENESS TRAINING

Implement an Employee Security Awareness Training Program to raise awareness for individuals responsible for handling money. Skyward Technology Solutions is a partner of KnowBe4, the leading Security Awareness Training program. For more information, visit:

SECURITY BEST PRACTICES

With today's sophisticated threats, it's essential to review your systems and take full advantage of built-in security features. To take a deep dive into security best practices for Skyward SMS 2.0 and Qmlativ, visit:

SECURITY TIPS

MULTI-FACTOR AUTHENTICATION

Use MFA to ensure only credentialed users are able to log in to your system:

Scan or search "Multifactor Authentication" in the Qmlativ Help Center.

SINGLE SIGN-ON

Save time while staying secure by configuring Single Sign-On for your applications:

Scan or search "SSO Launch Kit" in the Qmlativ Help Center.

SECURITY GROUP IP RESTRICTIONS

Limit access to secure resources with IP address range restrictions:

Scan or search "IP Address" in the Qmlativ Help Center.

UNAUTHORIZED ACCESS

Use the guides below to learn how to run reports to identify potential unauthorized access to Qmlativ Student and Business resources.

QMLATIV STUDENT GUIDELINES

QMLATIV BUSINESS GUIDELINES

Business Email Compromise Resources

Skyward Security Best Practices→ https://www.skyward.com/blogs/skyward-insider/2024/september/skyward-security-best-practices

CISA: K12 Guide → https://www.cisa.gov/k-12-school-security-guide

FBI: Report BEC Incidents → https://www.ic3.gov/

FBI: BEC Tips → https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/business-email-compromise

WI DPI: Cyber Security Resources → https://dpi.wi.gov/cyber-security/cyber-security-resources





Skyward's IT experts have the latest knowledge on industry trends and developments to help keep your network running smoothly.

NETWORK CONSULTING

- Resilient Wired Network Infrastructure
- Complete Wireless Network Solutions
- Virtual Server Design and Support
- Storage Area Network Solutions
- IP Telephony Solutions

SUPPLEMENTAL IT STAFFING

- Onsite and Remote IT Support
- Network Assurance Services

ASSESSMENT SERVICES

- Network / Security
- Disaster Recovery
- Secure Cloud Computing

SKYWARD OPTIMIZATION

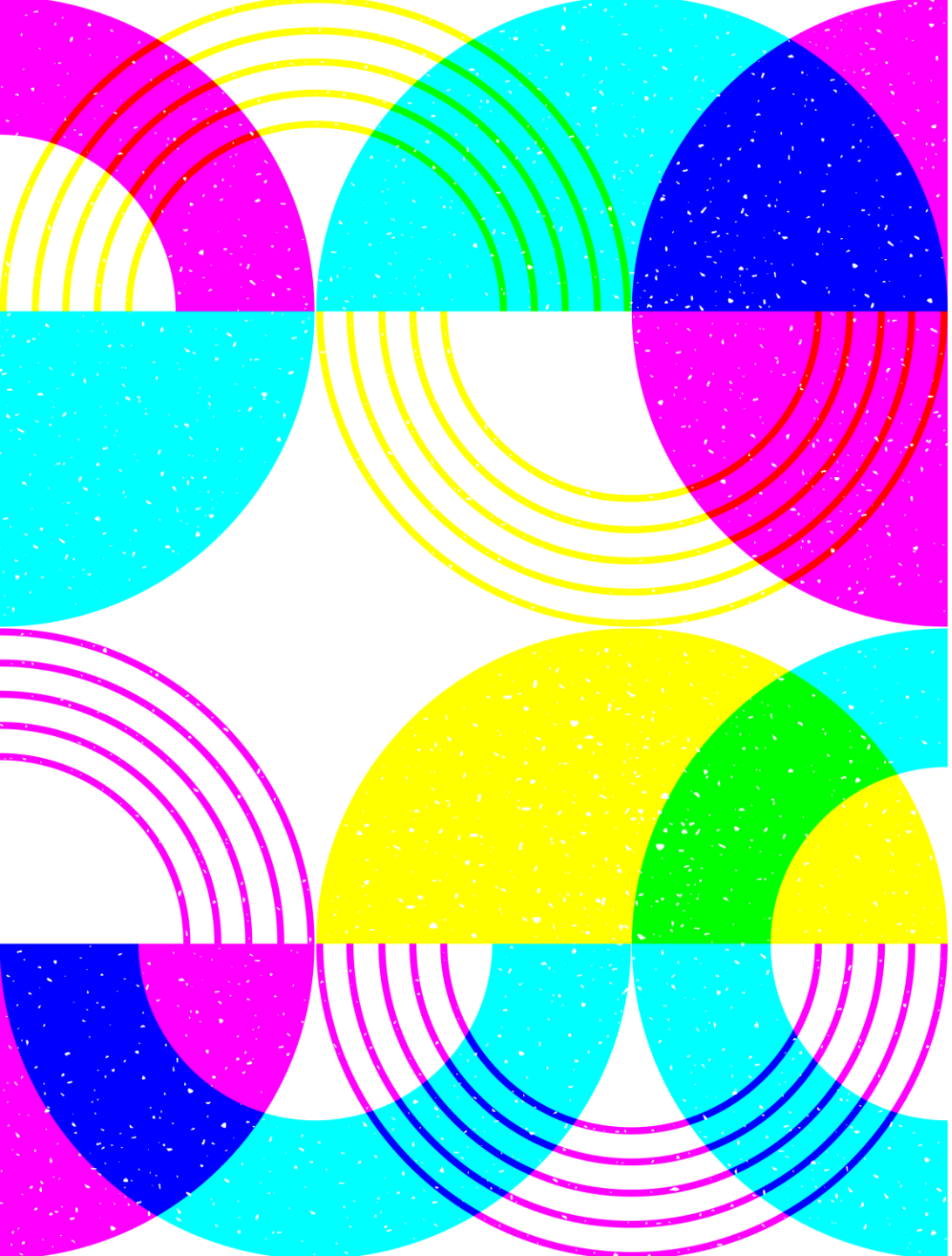
- Managed Services
- Database Tune-ups
- Remote Update Services
- System Admin Training

NETWORK SECURITY SOLUTIONS

- Intrusion Detection, Prevention, and Next Generation Firewalls
- Email Filtering, Archiving, and Security Solutions
- Internet Filtering and Monitoring Solutions
- On-Staff Security Experts

DISASTER RECOVERY SERVICES

- Skyward Disaster Recovery from ISCorp
- Onsite Data Center Disaster Recovery Solutions



SKYWARD®

iCON

thank you!