



FoxPointe Solutions

INFORMATION RISK MANAGEMENT

488 Madison Ave. 23rd Floor, New York, NY 10022

foxpointesolutions.com | 844.726.8869

Benefit Clerks Fall Training

Carl Cadregari, CISA, CCSFP,
CISO

FoxPointe Solutions

October 2024

PARTNER
OFFICE
SERVICE
EXCELLENCE
INDUSTRIAL

Cyber News



- Change Healthcare breached, 1 in 3 healthcare claims in the US effected.
- Late Discovery: CMS and Wisconsin Physicians Service Insurance Corporation notify 947k of last year's MOVEit data breach
- Two providers in Colorado and Alabama report breaches, and a benefits administrator in Georgia also reports a cyberattack
- American Family Insurance to notify 283,734 of breach linked to unemployment benefits fraud
- HHS Office for Civil Rights Imposes a \$240,000 Civil Monetary Penalty Against Providence Medical Institute in HIPAA Ransomware Cybersecurity Investigation
- Senate bill pushes cyber mandates for medical industry in wake of Change Healthcare debacle



INFORMATION RISK MANAGEMENT

• A Division of The Bonadio Group •

Why Data Security

Internet Reports

- As of today, there are 5.1 **billion** internet users
- There are 7.26 billion unique mobile users in the world today
- Savvy attackers are using increased levels of deception and, in some cases, hijacking organizations' own infrastructure
- 60 percent of all targeted attacks struck small- and medium-sized organizations
- All 50 States now have data breach statutes



Why Data Security

Open Enrolment

Data breaches are a constant threat, and open enrollment periods are a time when large amounts of data are being transferred, making them a target for hackers. Here are some tips to keep your data safe during open enrollment:

- Back up data regularly
- Make sure your data is stored securely and that you can restore it if needed.
- Security should be a priority all year, but take extra precautions during open enrollment.



INFORMATION RISK MANAGEMENT

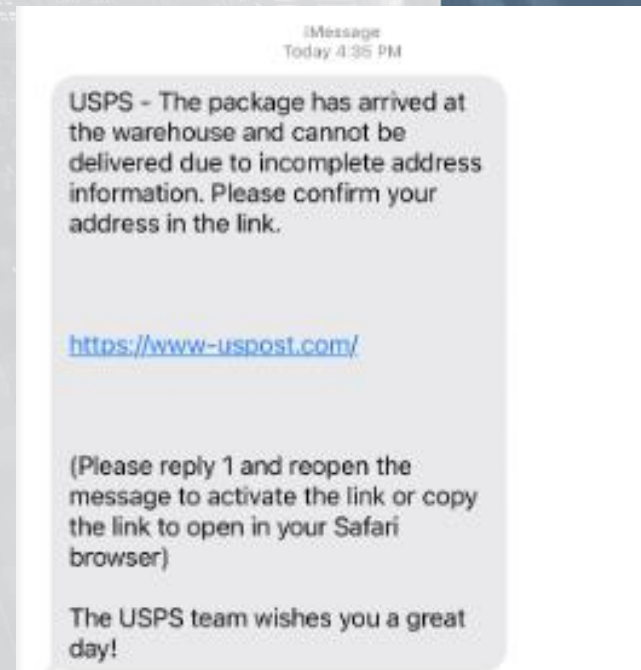
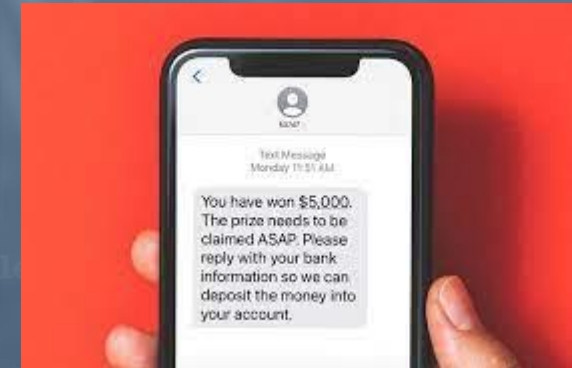
• A Division of The Bonadio Group •

Emerging Threats

Smishing

- Smishing is a form of phishing that uses **mobile phones** as the attack platform. The criminal executes the attack with an intent to gather personal information. Smishing is implemented through text messages or other SMS communications.

COINBASE: A withdrawal has been attempted from a new device. If this was not you, follow the steps here: <https://cbsupport.smsb.co/1HVFfA>



Data Protection Tools

- Email

- Don't use the free version – they are not secure or compliant with any data security law
- Make sure any “rules” are reviewed
- Use the “App” vs the “Browser” version



INFORMATION RISK MANAGEMENT

• A Division of The Bonadio Group •

Data Protection Tools

- Encryption
 - On all computers
 - On all portable devices
 - On email
- Passwords
 - Use Passphrases and MFA

Key Items



- Be skeptical
- Be aware of your online presence
- Inspect
- Don't click links
- Be smart with your passwords
- Keep your software updated
- Be an active part of your security strategy
- Risk assessment is NOT a one and done!



INFORMATION RISK MANAGEMENT

• A Division of The Bonadio Group •



FoxPointe Solutions

INFORMATION RISK MANAGEMENT

488 Madison Ave. 23rd Floor, New York, NY 10022

foxpointesolutions.com | 844.726.8869

Questions?