CYBER FRAUD AND SECURITY

Marty Malloy and Monica Schraml M3 Insurance

May 20, 2021

SERVING WISCONSIN PUBLIC SCHOOLS

Serving 250+ Wisconsin School Districts and counting...

SPECIALIZED SERVICE SUPPORT FOR SCHOOLS

- Student & Staff Mental + Physical Health

- Talent Attraction + Retention

- School Safety

- Active Shooter Trainings

- Vendor Summits

M3 INSURANCE

AGENDA

Part 1: Schools are Targets

Part 2: Risk Management

Part 3: Post Breach Recovery

PART ONE

Schools Are Targets

CYBERSECURITY STATISTICS

- 1,232 school data breaches were disclosed in the U.S.
- A new cybersecurity incident strikes K-12 Schools nearly three times daily
- 2020 Record breaking year for school cyber attacks
  - https://thehill.com/policy/cybersecurity/542518-new-research-finds-record-breaking-number-of-k-12-cyber-incidents-in

M3 INSURANCE

CYBERSECURITY STATISTICS

- K-12 schools experienced 1,232 publicly reported cybersecurity incidents in 2018. 60% resulted in students' personal data being compromised
- Nearly 60 million Americans have been affected by identity theft

2021 HEADLINES

- Business email compromise: school loses $1.8 million
- Phishing campaign: school loses $1.1 million
- Telephone transfer fraud: school loses $885,000
- Email transfer fraud: school loses $690,000
- Wire transfer fraud: school loses $550,000

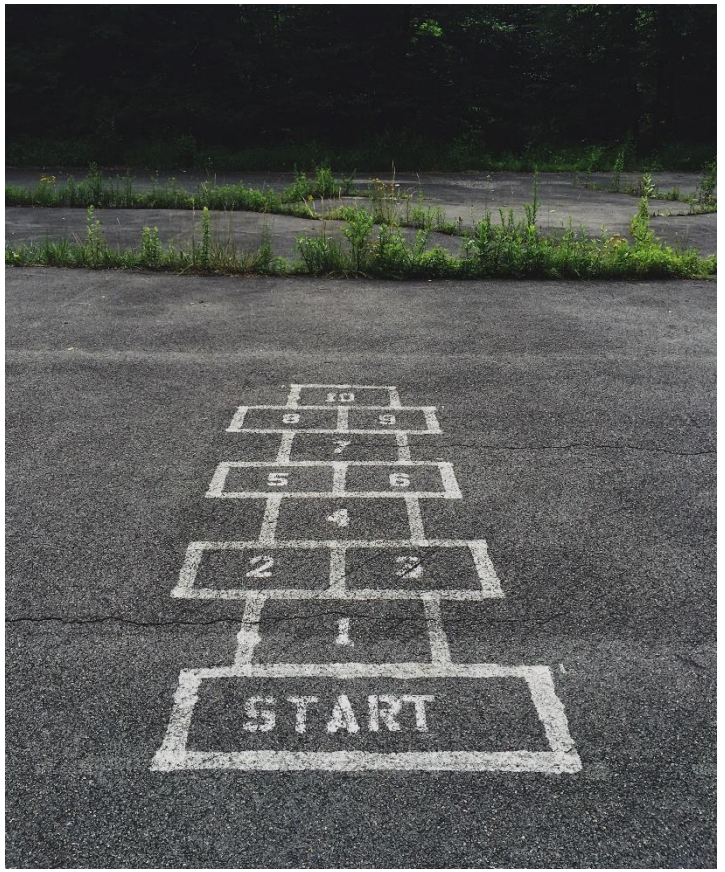
POTENTIAL NEW REGULATORY RULES

ALREADY IN EFFECT IN SEVERAL STATES

- It may be considered an unfair and deceptive act or practice if you handle consumer data and your organization does not have appropriate safeguards in place. Fines of $750-$1,000 per record

WHY SCHOOLS ARE TARGETED

- Young internet users without knowledge of current methods for data breaches (i.e. phishing, ransomware, etc.)
- Personal devices connecting to school network
- Schools less likely than businesses to have cyber loss prevention plans

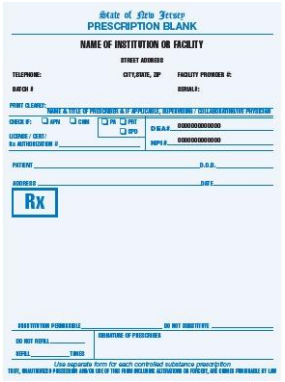


WHY SCHOOLS ARE TARGETED

- Employee cyber training is expensive
- Multiple access points
- Budget for cyber security is not always a priority

DATA: WHY SCHOOLS ARE TARGETED

- HIPAA – student and staff health data is at risk.
- Most valuable data to cyber criminals
  - Personal Health Information
  - Payment Card Information
  - Youth Data
    - *A false identity set up for a minor may not be discovered until that minor turns 18*



HOW: SOCIAL ENGINEERING

The use of deception to:

- Manipulate individuals into divulging confidential information for fraudulent purposes
- Misdirect and steal money
- Manipulate a website commonly used by a district divulge information for fraudulent purposes

HOW: SOCIAL ENGINEERING

Gathering usernames, passwords, private emails, and business email addresses through:

- Fake websites
- Website skimming
- Fake SMS messages
- Phishing emails

HOW: SOCIAL ENGINEERING

- Phishing Emails
- Vishing (Voice Phishing)
- SMShing (Text Phishing)
- WaterHoling
- Tailgating

PART TWO

Risk Management

PREVENTATIVE MEASURES

- **Passwords**
- **Multi Factor Authentication**
- **Employee Awareness**
- Cyber Security Committee
- Patching
- Log Data *(Microsoft 365)*

M3 INSURANCE

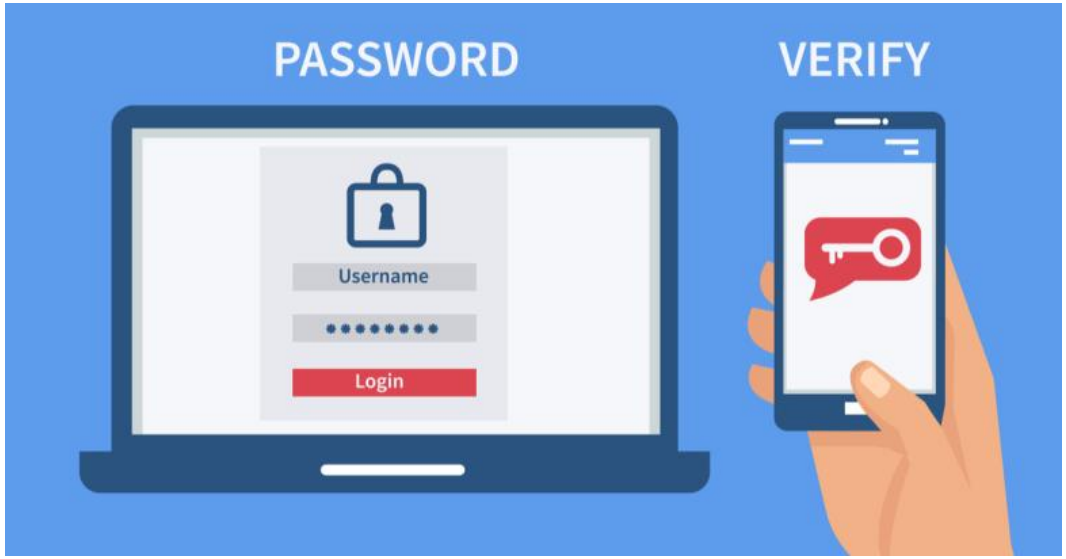
PASSWORDS

We are all terrible at passwords…

- We use passwords that are easy to guess
- We use re-use passwords across many sites

MULTI FACTOR AUTHENTICATION

- Text Verification
- Push Verification
- Biologic
  - Fingerprint
  - Face recognition



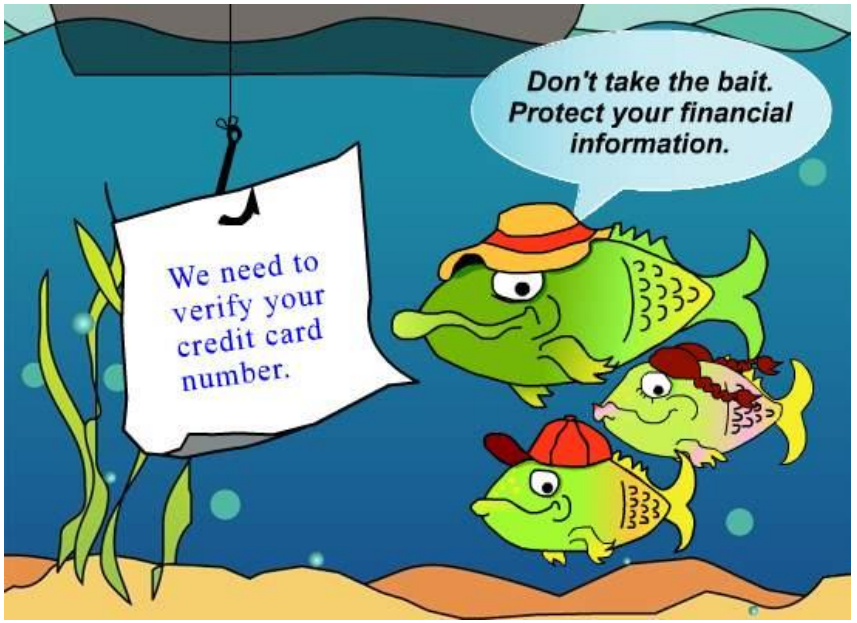
PASSWORDS

Password best practices

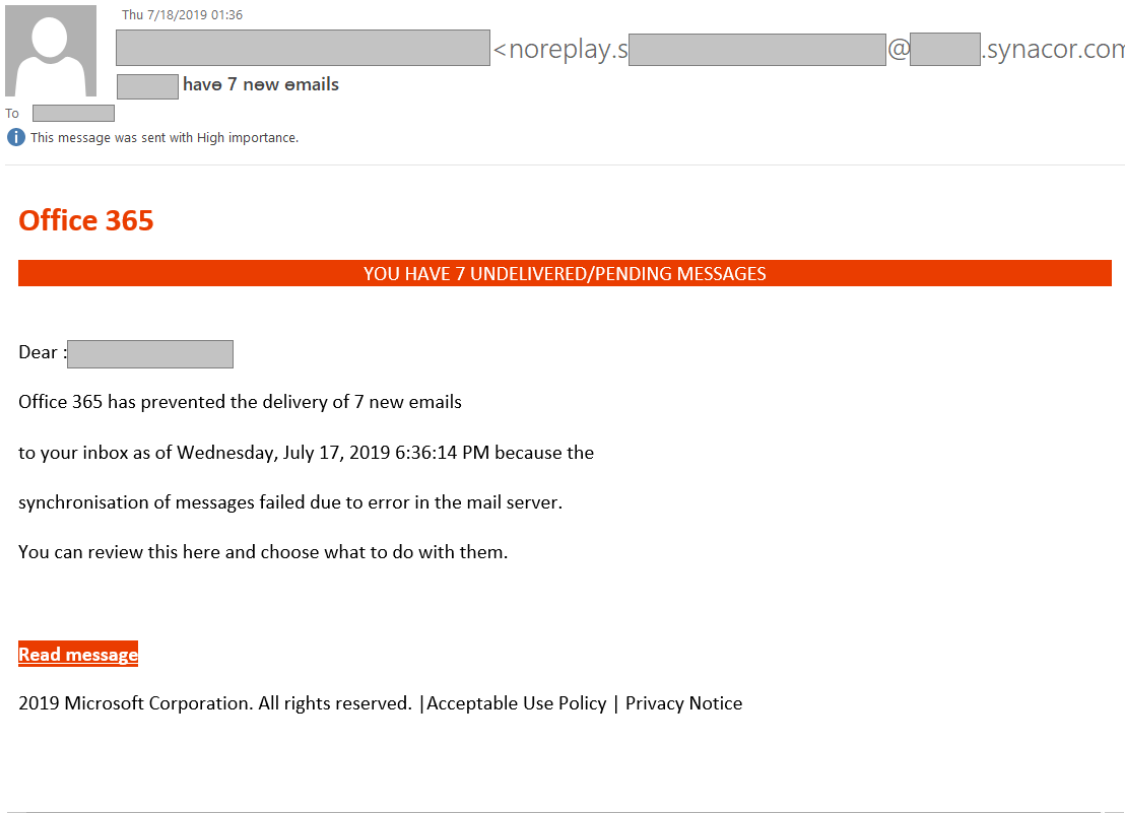
- 16 characters – different for each site (Use Phrases!)
- Change annually
- Use two factor

EMPLOYEE AWARENESS: 8 SIGNS OF PHISHING

- Unfamiliar tone/greeting
- Grammar and spelling errors
- Inconsistencies in email address, links, and domain names
- Threats or urgency
- Suspicious attachments
- Unusual request
- Short and sweet
- Request for credentials, payment info or personal details



EMPLOYEE AWARENESS: PHISHING EMAIL



Thu 7/18/2019 01:36

[redacted] <noreplay.s[redacted]@[redacted].synacor.com

[redacted] have 7 new emails

To [redacted]

This message was sent with High importance.

Office 365

YOU HAVE 7 UNDELIVERED/PENDING MESSAGES

Dear : [redacted]

Office 365 has prevented the delivery of 7 new emails

to your inbox as of Wednesday, July 17, 2019 6:36:14 PM because the

synchronisation of messages failed due to error in the mail server.

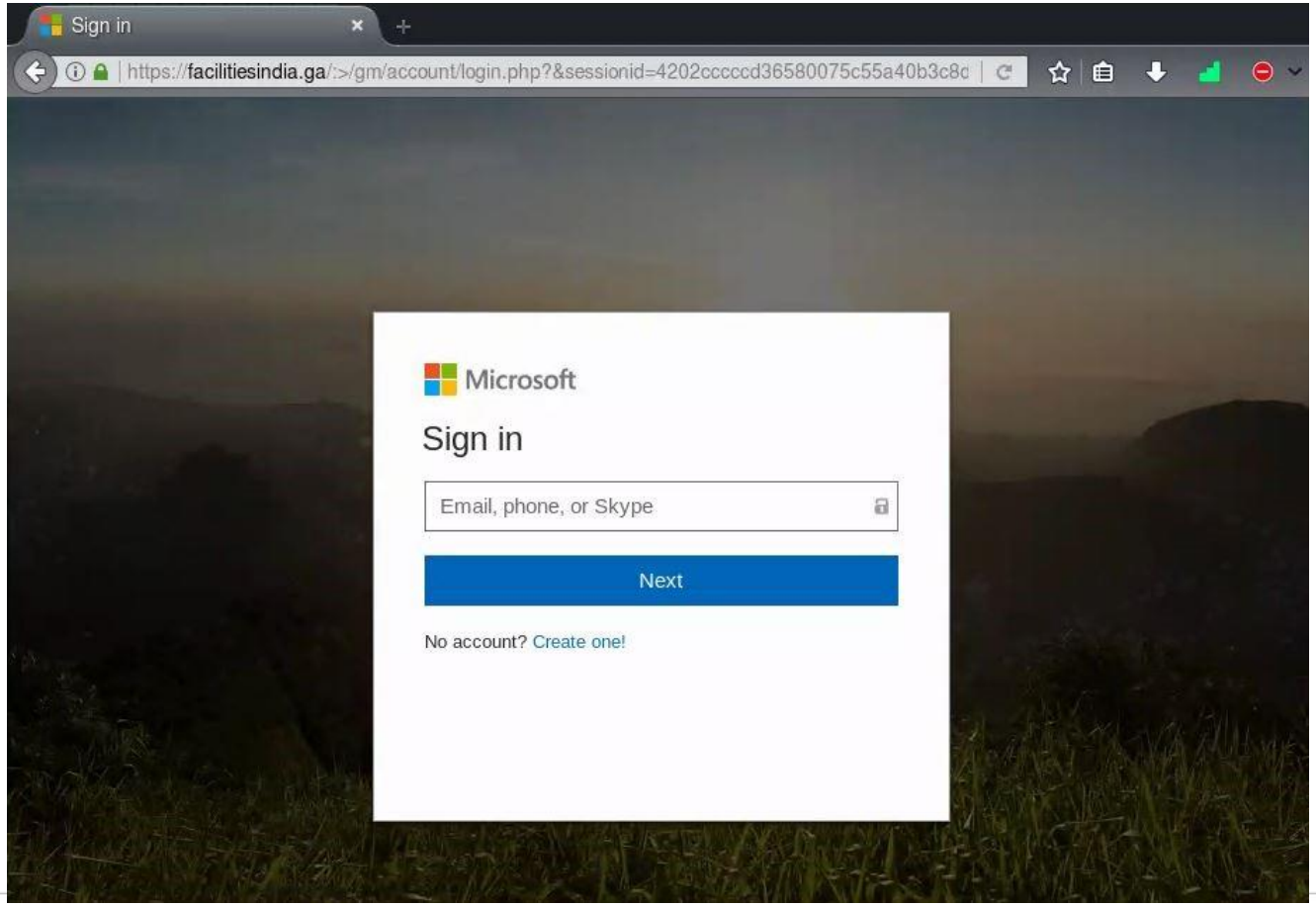
You can review this here and choose what to do with them.

Read message

2019 Microsoft Corporation. All rights reserved. |Acceptable Use Policy | Privacy Notice

INSURANCE

EMPLOYEE AWARENESS: A COMPROMISED SITE



PART THREE

Post Breach/Recovery

RECOVERY

INCIDENT RESPONSE – DO'S

- Have a written plan
- Test your written plan
- Contact your insurance representative (if applicable)
- Alert all applicable leadership (see written plan)

RECOVERY

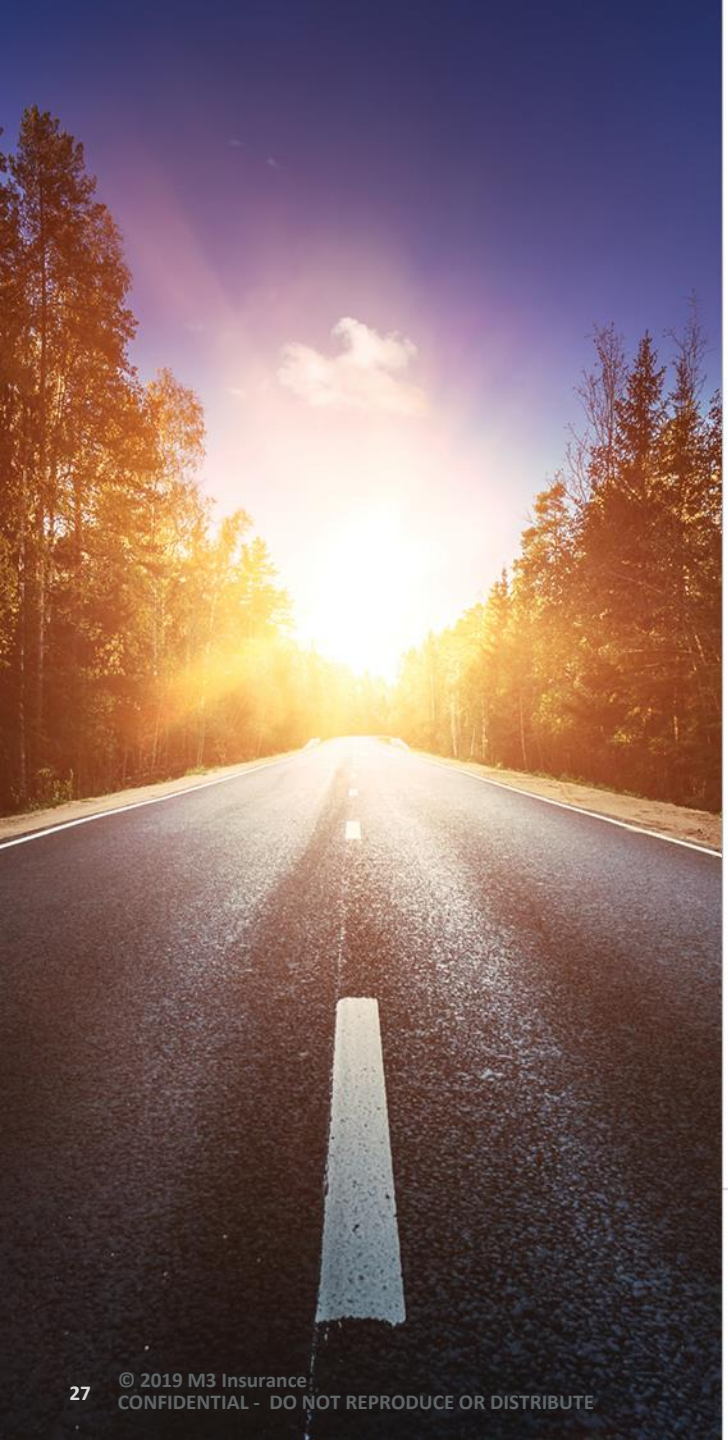
INCIDENT RESPONSE – DON'TS

- Allow your internal IT or Outsourced IT to try and "fix" the problem
- Hire third parties without consulting your insurance company
  - If you are insured you must use approved vendors
    - *Legal*
    - *Forensics*

RECOVERY

INCIDENT RESPONSE – DON'TS-If Uninsured ☹

- Alert customers or outside parties without consulting legal (even if obligated to under specific time frame)
- Assume your corporate inside/outside counsel is experienced in data breaches



STAY UP TO DATE

The **M3 Insight Center** is packed with posts to help you make the right decisions for your district. Topics include:

- Self Care Isn't Selfish: Help Employees Prioritize Wellness
- Risk Management Strategies for Combative Students
- Public Entities: On the Front Lines of Cyber Exposure

Subscribe to the M3 Insight Center to receive valuable notifications directly in your inbox.