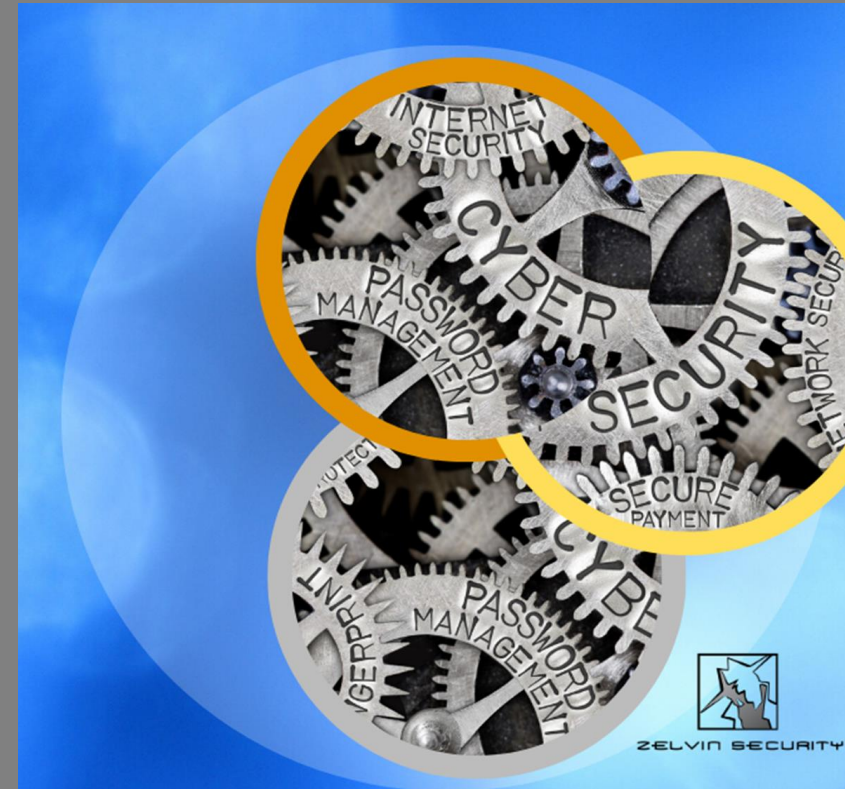


# Slow the Spread of Cyber Criminals and the NYS SHIELD ACT

Hacking\_Your\_Business  
Is\_Our\_Business

Presented by  
**ZELVIN SECURITY**





"Don't put off until tomorrow  
what you can  
do today."

BENJAMIN FRANKLIN

**SLOW THE  
SPREAD OF  
CYBER  
CRIMINALS**



## THE “COVID DISRUPTER”



# MAKING FRIENDS WITH TECHNOLOGY



# Endless Opportunities



This Photo by Unknown Author is licensed under [CC BY-SA-NC](#)



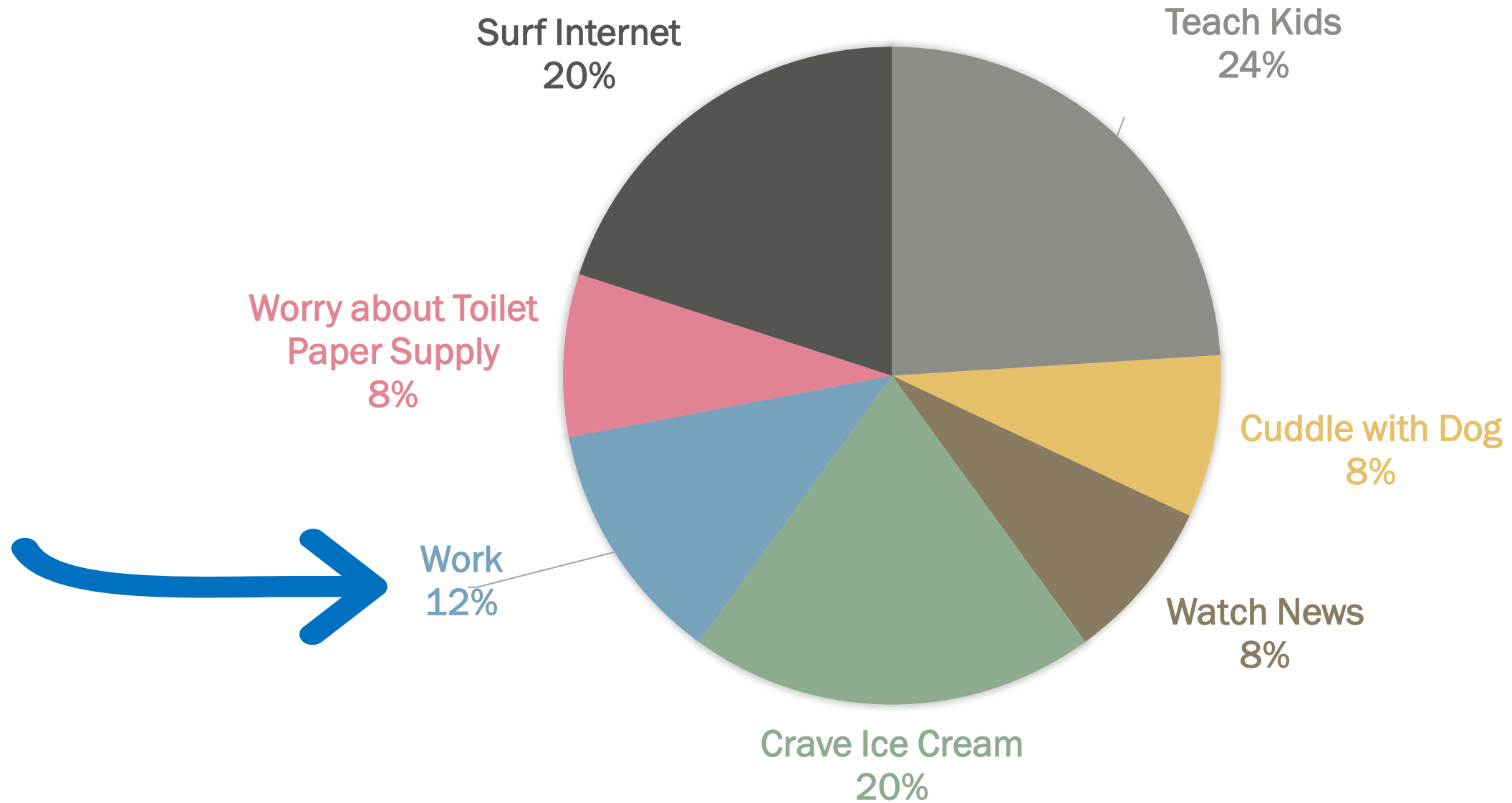
*“ We need to verify  
your banking  
information to send  
you federal stimulus  
payments. “*



## HOW TO SPOT A SCAM



# ALLOCATION OF TIME WHEN WORKING FROM HOME





# CREDENTIAL STUFFING

Username  
dexter

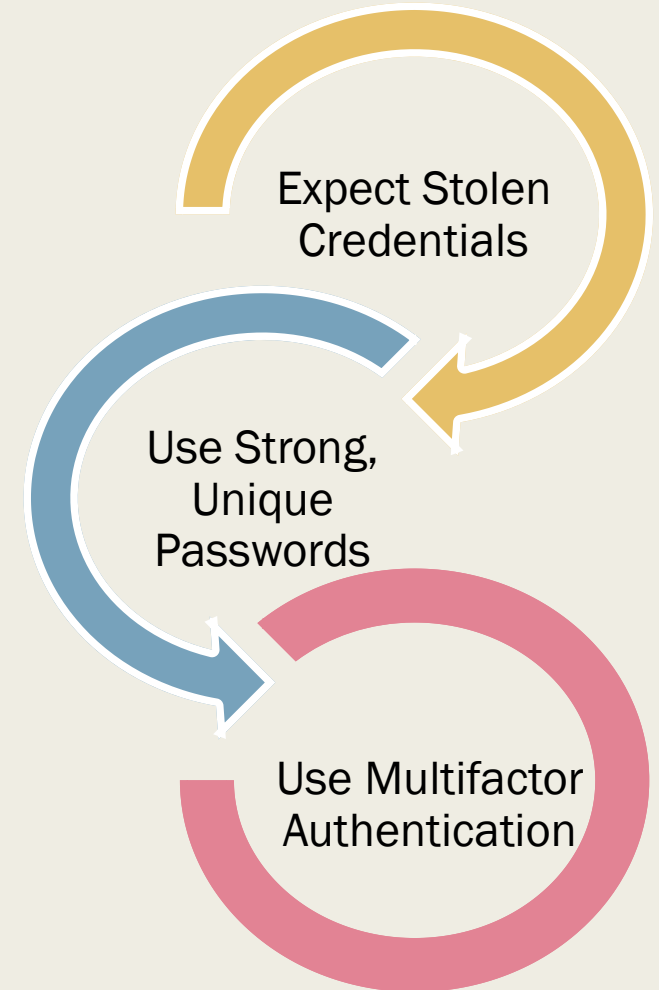
Password  
.....

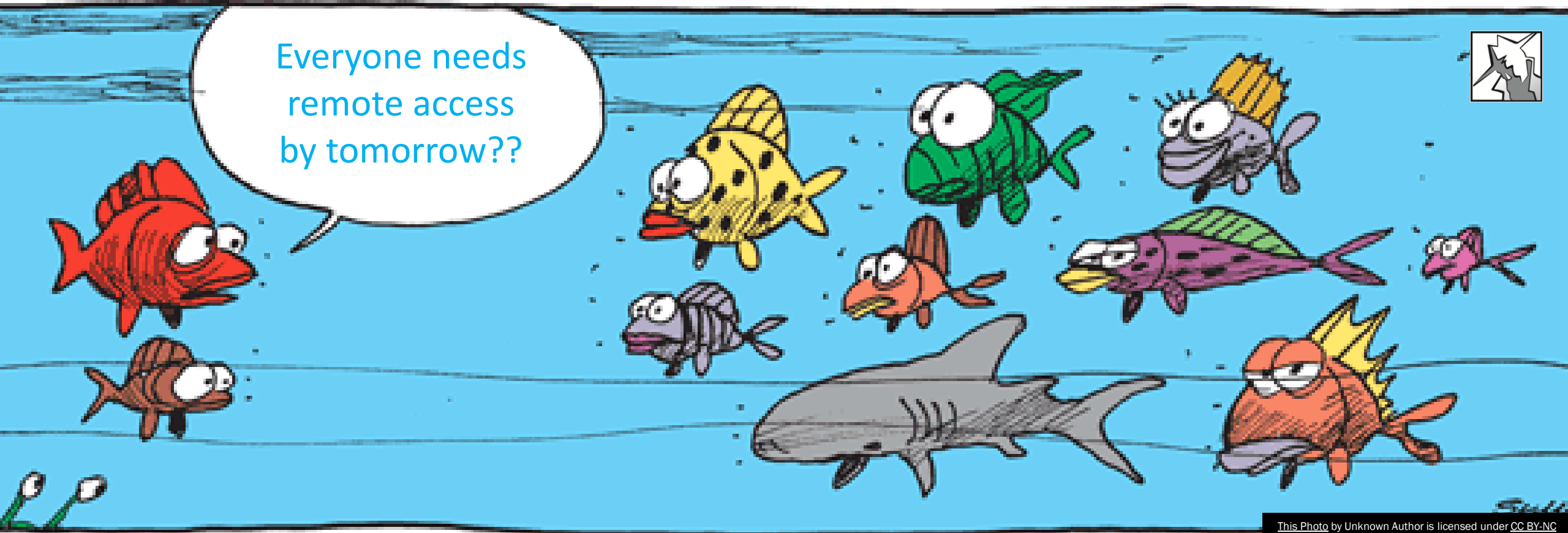
☐ Remember Me

Username  
dexter

Password  
p@\$5w0rd

☒ Remember Me





This Photo by Unknown Author is licensed under CC BY-NC

SUPPORTING A REMOTE TEAM USING TECHNOLOGY



This Photo by Unknown Author is licensed under [CC BY-NC-ND](#)

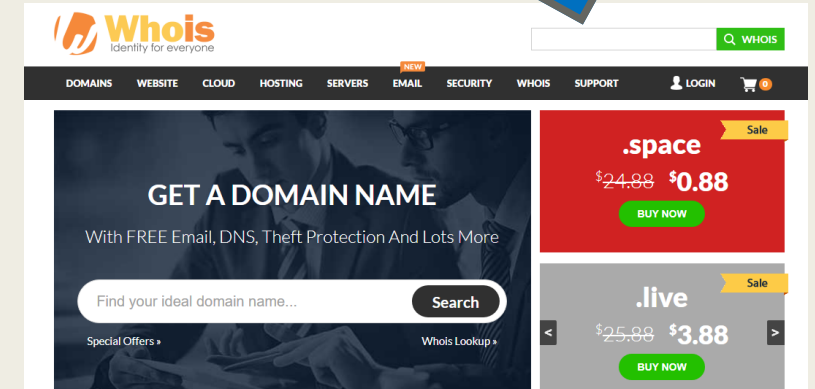
SUPPORTING YOUR REMOTE PEOPLE

# Sample Educational Memo to Staff

Cybercriminals are using the coronavirus to send phishing emails to people around the world. If you receive an email that looks legitimate **DO NOT CLICK** on the link in the email. Instead, open your browser and search for information about the topic described in the email. Only go to sites ending in .edu or .gov for primary source resources. There are many sites online that look like the COVID-19 the CDC, WHO, Johns Hopkins University, IRS, your bank and so many more. These sites may contain malware or attempt to direct you to a malicious site.

If you have a question about the authority or owner of a website visit: Whois.com

<https://coronavirus.jhu.edu/map.html>



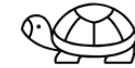
Domain Name: JHU.EDU

Registrant:

Johns Hopkins University  
5801 Smith Avenue  
Suite 3110B  
Baltimore, MD 21209  
USA

# Sample: Educational Memo to Staff

Cybercriminals are seizing the opportunity of the distractions of the coronavirus by sending phishing emails and soliciting private information. We realize that you may find yourself more distracted “at work” these days and looking for information about the virus, the guidelines for quarantining, and testing options. It’s normal to want to learn more; however, we ask that you follow these simple rules to protect your digital assets:



## SLOW DOWN

Think before you click. Criminals rely on urgency and secrecy.



## CALL TO VERIFY

If you're not expecting the email...don't click on links or take action until you've spoken with the sender personally.



## TRUST NO ONE

Zero Trust- Be suspicious of phone calls, emails, visitors. Assume it is malicious unless otherwise verified. Assume all links and attachments are dangerous.



## RECOGNIZE PHISHING IDENTIFIERS

Verify an email is authentic and the sender is true *before* clicking.



**Analyze** the message and subject line.

Don't trust the **display name**.

Check for **spelling mistakes & erroneous spacing**.

Check grammar- **Is it poorly written?**

Question **why** you're receiving a link or attachment.

Beware of urgent messages or perceived security.

If you panic after reading the message...**think twice** before clicking.

**Review the signature** for inconsistencies.

**Do not confirm personal information** using the method provided

# Sample: Educational Memo to Staff

Cybercriminals are seizing the opportunity of the distractions of the coronavirus by attempting to gain access to online activities using home routers.

Your home Wifi router should have a lengthy, unique passphrase and you should have a router using the most current software version.

If you have questions please call the help desk at...



# Sample: Educational Memo to Staff

While working from home we ask you to follow the same cyber security practices as you do in the office

**Log out** of your computer when you are not at your desk.

**Only approved users** should use your computer and only perform work activities on our company issued device.

**Please refrain from** using your company asset for non-work related internet browsing, games, music, recipes, and more.

Thank you!



[This Photo](#) by Unknown Author is licensed under [CC BY-NC-ND](#)



[This Photo](#) by Unknown Author is licensed under [CC BY-SA](#)

# Sample: Educational Memo to Staff

At Company XYZ, we are here to support your efforts as you work from home. If you have an IT related issue please DO NOT HESITATE to turn to IT for support.

**We are never too busy to help you** with your VPN Connection, questions about the legitimacy of an email or website, issues about your machine's performance, and the necessary updates (software upgrades) on your computer, smartphones and tablets.





SUPPORTING YOUR REMOTE PROCESS



It's not IF a cyber-attack  
will happen, it's about  
WHEN it will happen.

ZELVIN SECURITY

SLOW THE  
SPREAD OF  
CYBER  
CRIMINALS AND  
VIRUSES



# NYS SHIELD ACT

Stop Hacks and Improve Electronic Data Security  
Amends Section 899-aa of the NYS General Business Law



# WHAT IS THE SHIELD ACT?

- Expands the definition of private information
- Expands the definition of a data breach
- Expands the security safeguards required
- Breach notification required
- Civic penalties in place for non-compliance

**Stop Hacks and Improve  
Electronic Data Security**

## NYS SHIELD ACT



### PROTECT DATA & PRIVACY

All businesses must protect NY resident's data regardless of the state they are domiciled. Fines for non-compliance are imposed by the NYS Attorney general.

# WHO DOES THE SHIELD ACT APPLY TO?

Any business or organization with

More than 50 employees

More than \$3M in annual revenue

More than \$5M in year-end assets

## Stop Hacks and Improve Electronic Data Security

# NYS SHIELD ACT



### PROTECT DATA & PRIVACY

All businesses must protect NY resident's data regardless of the state they are domiciled. Fines for non-compliance are imposed by the NYS Attorney general.

Private Information is expanded under the law to include SS#, driver's license #, account #, password, bio-metric data, username, security question answers, and more.

What is considered  
Private Information?



## ADMINISTRATIVE

The business must appoint one central cyber security leader who manages the security awareness training program for employees and a robust vendor security program holding partners to high security safeguards by contract.



## TECHNICAL

The business must perform proactive cyber security tests (Penetration Tests) of the network and software. And, businesses must detect, prevent and respond to attacks. (Threat Monitoring). Zelvin Security can help you with this control.



## PHYSICAL

Businesses must not hold onto private information longer than it is needed and they must protect data at rest, in storage, during transition, from unauthorized physical access and at disposal or at the sale of the business.

# What Does the Shield Act Require?



**Civil Penalties for  
violating the law:  
Maximum: \$250k  
Minimum: \$20 per  
record or \$5k.**

**Stop Hacks  
and Improve  
Electronic  
Data Security  
(SHIELD) Act  
for NYS**

**NYS Shield Act Effective March 21, 2020**

**Fines and Breach  
Notification Guidelines**

## Stop Hacks and Improve Electronic Data Security

# NYS SHIELD ACT



### APPLIES TO BUSINESSES

More than 50 employees, more than \$3M annual revenue in the last three years, or less than \$5M in year end total assets.

Compliance is achieved when state or federal regulatory agency considers the business compliant. State of domicile is not a factor.

### SECURITY CONTROLS REQUIRED

The SHIELD Act requires a business to apply reasonable security safeguards using Administrative, Technical and Physical Security Controls to realistically and practically protect the data it receives of all NY residents. All businesses with 50 or more employees or more than \$3M in annual revenue must comply with this NYS Law.



### ADMINISTRATIVE

The business must appoint one central cyber security leader who manages the security awareness training program for employees and a robust vendor security program holding partners to high security safeguards by contract.



### TECHNICAL

The business must perform proactive cyber security tests (Penetration Tests) of the network and software. And, businesses must detect, prevent and respond to attacks. (Threat Monitoring). Zelvin Security can help you with this control.



### PHYSICAL

Businesses must not hold onto private information longer than it is needed and they must protect data at rest, in storage, during transition, from unauthorized physical access and at disposal or at the sale of the business.

# LEARN MORE AT ZELVIN.COM

AS OF MARCH 2020 THE  
SHIELD ACT IS NYS LAW  
Learn More at [www.Zelvin.com](http://www.Zelvin.com)

(607) 758-9427



ZELVIN SECURITY

We are  
never done  
getting better...

ZELVIN SECURITY

## Educational Resources:

SANS Resources  
CISOMag.com  
Krebsonsecurity.com  
RSA  
Staysafeonline.org  
CSIAC.org  
ITS.NYS.GOV  
K12cybersecure.com

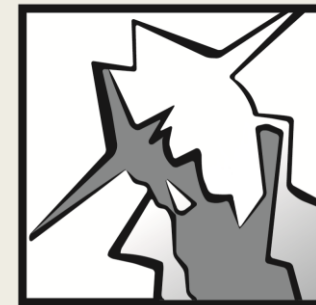


Thank You!

# Questions?

ZELVIN SECURITY

Since 2002  
Cortland, NY  
Zelvin.com



ZELVIN SECURITY  
zelvin.com