

*CyberSecurity attacks cannot be prevented completely but the frequency and impacts can be managed better.*

# Cyber Security 101

*Understanding Cyber  
Security Problems*

*And How to Avoid Them*





Data security means protecting digital data, such as those in a database, from destructive forces and from the unwanted actions of unauthorized users, such as a cyberattack or a data breach.

# Security Goals

The security goals for information systems involve:

- **Confidentiality** - kept private where needed
- **Integrity** - can be relied on for accuracy
- **Availability** - there when you need it
- **Resilience** - endures adverse scenarios

# FAMILY EDUCATIONAL RIGHTS & PRIVACY ACT



FERPA  
VIDEO ONE

# K-12 Cyber Security Challenges

In a K-12 education environment several factors shape our approach to addressing Cyber Security:

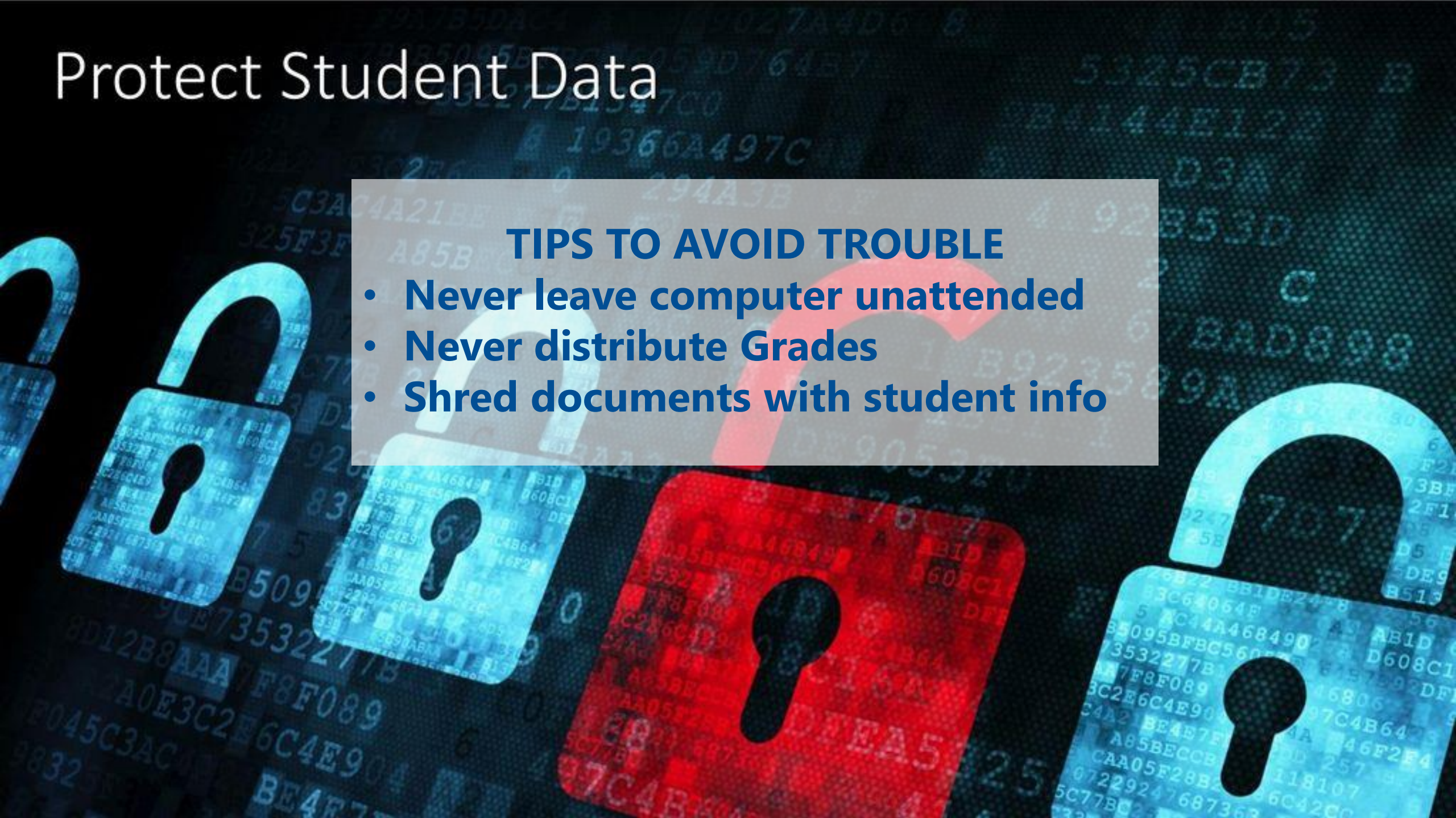
- Legal statutes governing student information privacy
- Non-profit nature of institutions
- Unclear roles and responsibilities



# Privacy Laws



- **FERPA** – Parents have a right to know what information is in their child's education record and they have a right to have it correct.
- **COPPA** – Online service providers can't ask for personal information of children under 13 without consent of the parent or appropriate others.
- **PPRA** – If you want to survey students and ask them sensitive/confidential questions, parents have a right to opt their student out.
- **HIPPA** (Health Insurance Portability & Accountability Act) – 1996 – US Dept. of Health & Human Services.
- **CIPA** – Requires K-12 schools and libraries using E-Rate discounts to limit children's exposure to pornography & explicit content online.



# Protect Student Data

## TIPS TO AVOID TROUBLE

- Never leave computer unattended
- Never distribute Grades
- Shred documents with student info

- **Never leave computer unattended**
- **Never distribute Grades**
- **Shred documents with student info**

- **Never leave computer unattended**
- **Never distribute Grades**
- **Shred documents with student info**



# **Terms & Conditions**

**1** rules and requirements that one agree to abide by in order to use a service; **2** general and special arrangements, provisions, requirements, rules, specifications, and standards that form an integral part of agreement or contract

I Agree

I Have No Idea  
What This Says

# Vetting Apps

<https://ikeepsafe.org/products/>

<https://privacy.commonsense.org/>

<https://secure2.cpsd.us/a4l/search.php>

# Data Security Important Terms

---

A **Vulnerability** provides the opening for an adversary but themselves represent no threat

---

A **Threat** exists when someone exploits a vulnerability with negative consequences

---

An **Incident** is an actual specific realization of a threat (also known as an **Attack**)

# Common Threats and Their Genesis

Hacking < Password  
compromised < Phishing

Malware < Exe Download  
< Careless people

DDoS < Planned Attack <  
You can buy one too!!





# Common Vulnerabilities

---

Uneducated users

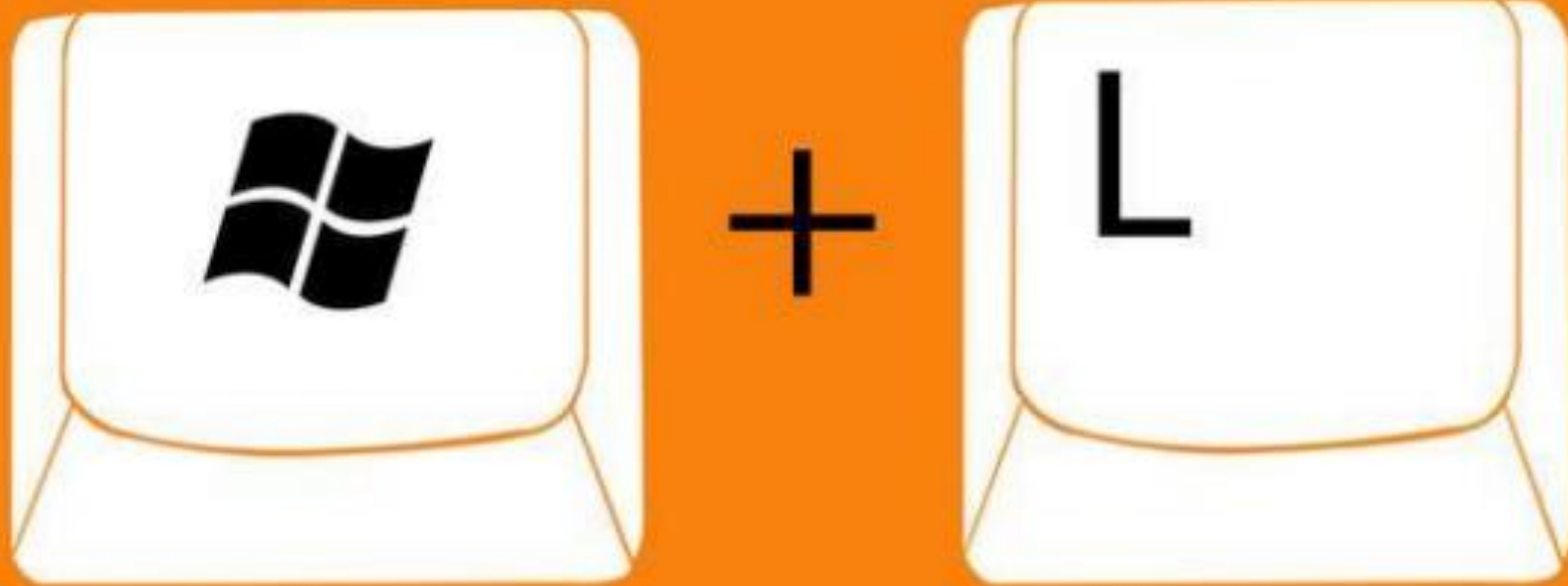
---

Bad password  
policies

---

Outdated security  
practices

# Lock your computer screen!



## LOCKS THE COMPUTER



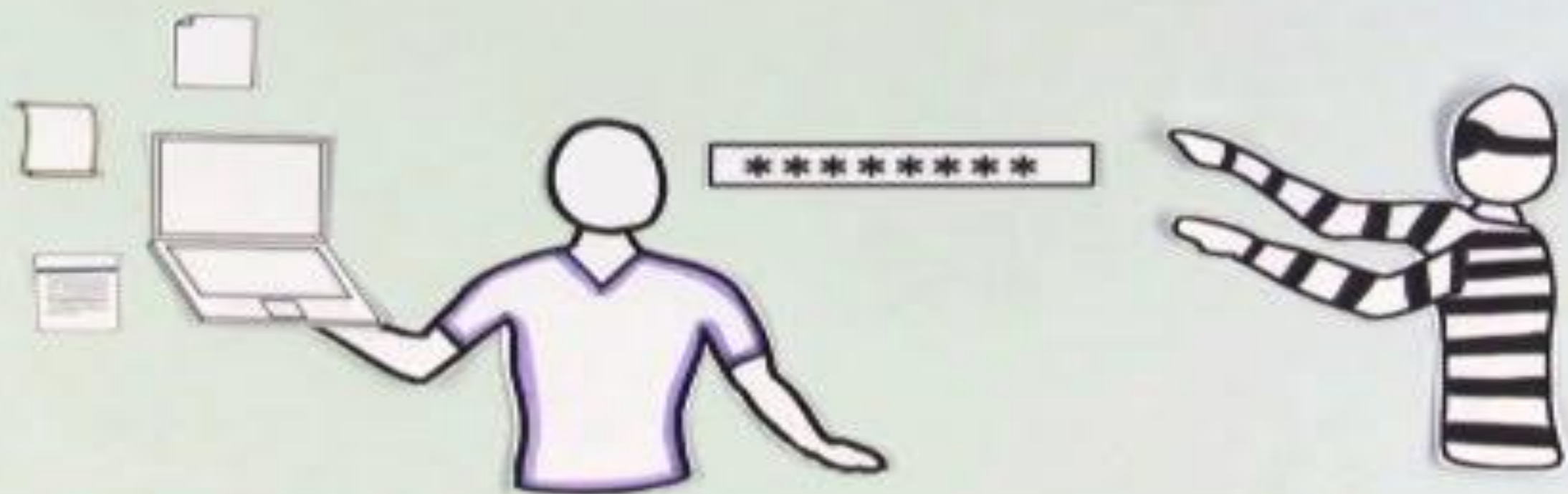
MAC User?

Q

control

command





# Creating a Password



Step 1	Pick two words.	
Step 2	ALL-CAPS the first word	
Step 3	Replace all vowels with 2	
Step 4	Replace the space with two # symbols.	
	<b>Password</b>	

# Password Template

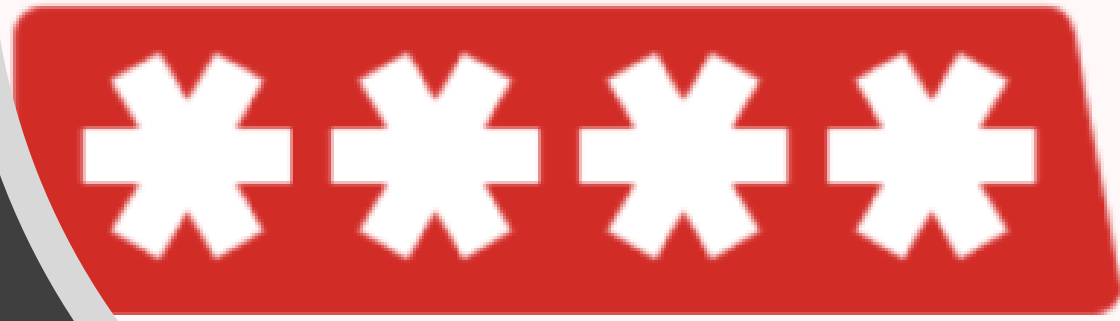
Step 1	Pick _____ words.	
Step 2	ALL-CAPS the _____ word	
Step 3	Replace the _____ with number _____.	
Step 4	Replace the space with _____ symbols.	
	<b>Password</b>	

***A strong password is one line of defense against hackers.  
Stay vigilant online!***

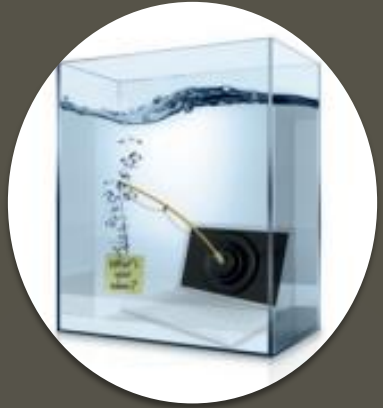
# Password Helper

- LastPass -  
<https://www.lastpass.com>
- Password Manager

LastPass







Phishing

Brute  
Force  
Attack



Drive by  
Download

Distributed  
Denial of  
Services  
(DDoS)



Advanced  
Persistent  
Threats



Ransomware

Cyber Threats Breakdown

# Phishing

Phishing refers to the process of deceiving recipients into sharing sensitive information with an unknown third party (cyber criminal).



# Phishing: Sources

- Websites
- Social Media
- Phone Calls
- Email



# Types of Phishing



BULK  
PHISHING

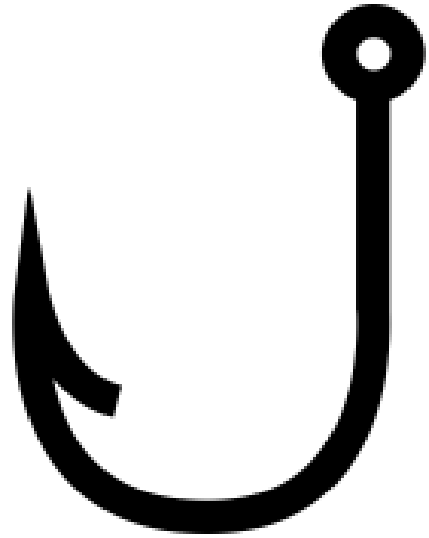


SPEAR  
PHISHING



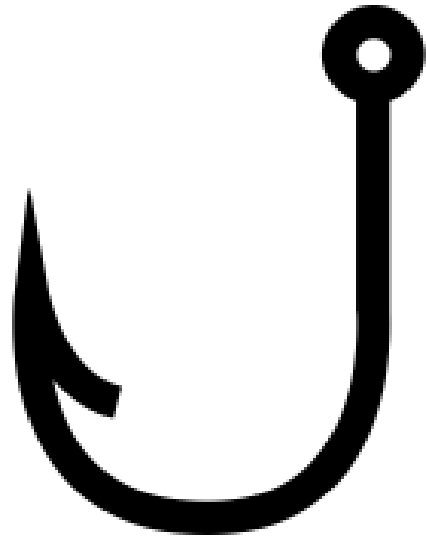
WHALING





## BULK PHISHING

- Widespread
- Generic
- Many Variances



# BULK PHISHING



**From:** Bank of America <crvdgi@comcast.net>  
**Subject:** Notification Irregular Activity  
**Date:** September 23, 2014 3:44:42 PM PDT  
**To:** Undisclosed recipients: ;  
**Reply-To:** crvdgi@comcast.net



### Online Banking Alert

Would be capitalized

**Dear member:**

We detected unusual activity on your Bank of America debit card on **09/22/2014**.  
For your protection, please verify this activity so you can continue making debit card transactions without interruption.

**Please sign in to** your account at <https://www.bankofamerica.com>

to review and verify your account activity. After verifying your debit card transactions we will take the necessary steps to protect your account from fraud.

<http://bit.do/ghsdfhgdsd>

If you do not contact us, certain limitations may be placed on your debit card.

Grammatical Error

© 2014 Bank of America Corporation. All rights reserved.

## Free Training

---



**Nathan Mielke** <mielkedata@gmail.com>

to nathan.mielke ▾

Hello

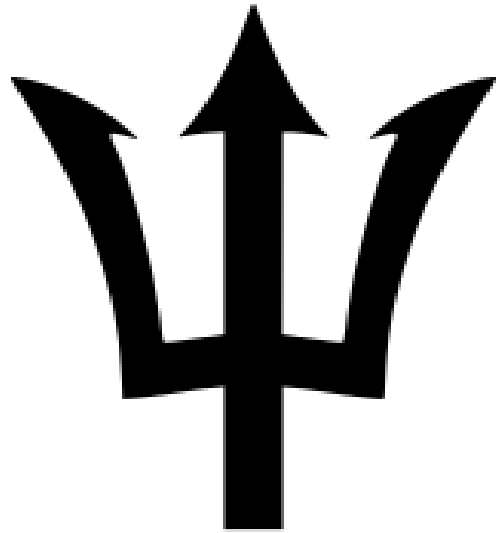
Click hear to enter your info to get free training

<http://bit.ly/2kvUGpE>



Nathan Mielke  
Hartford Union High School  
Technology Services  
[262.670.3236](tel:262.670.3236)

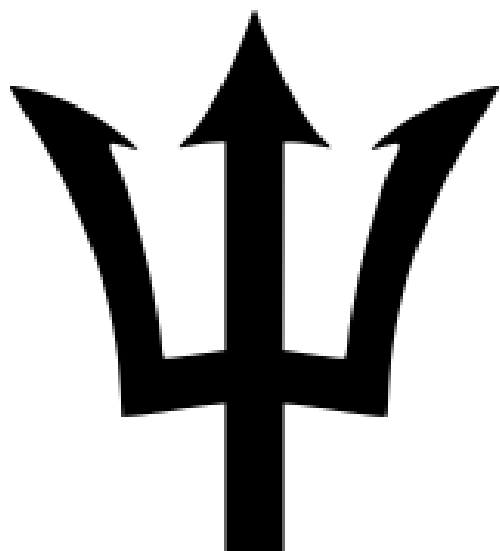
---



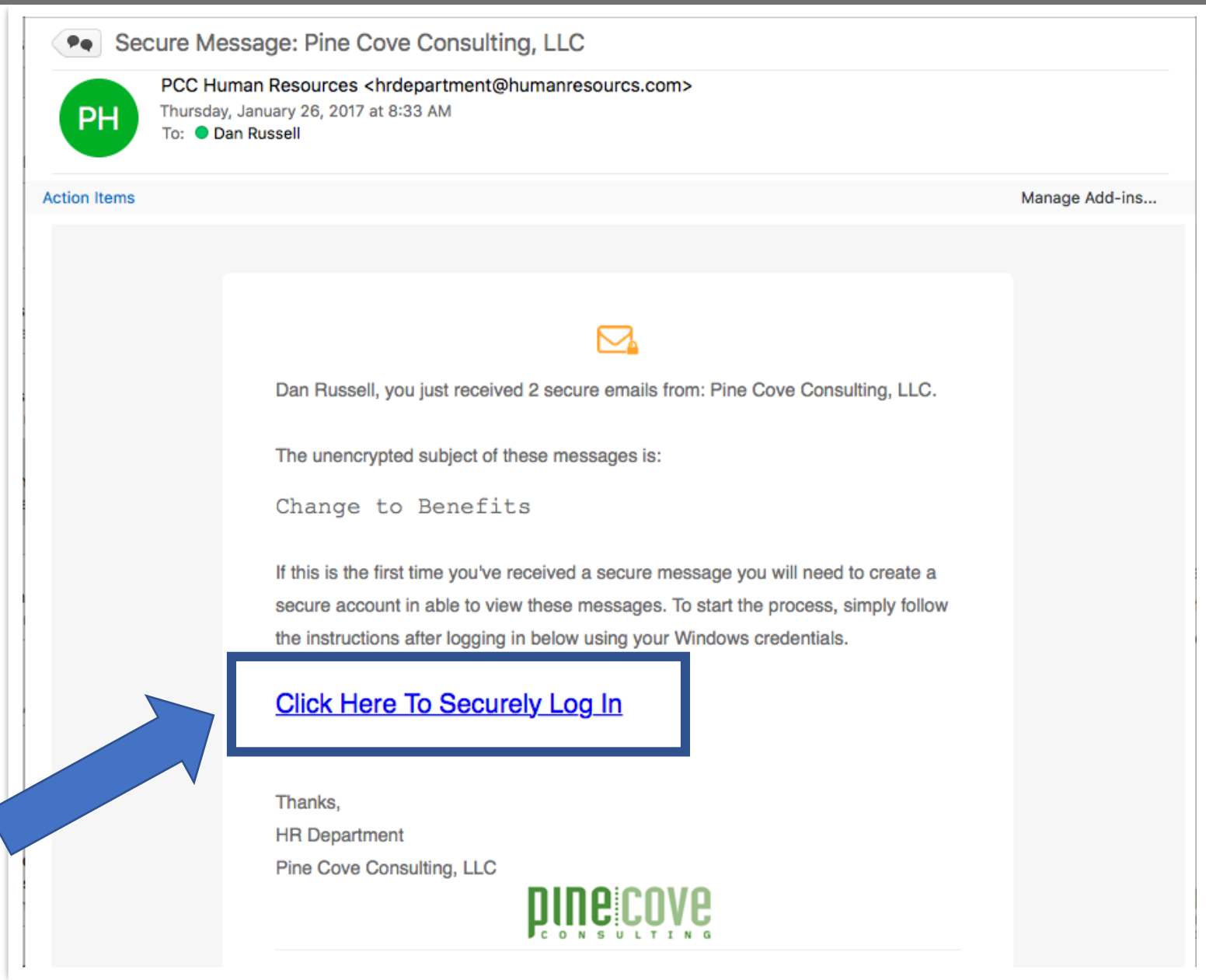
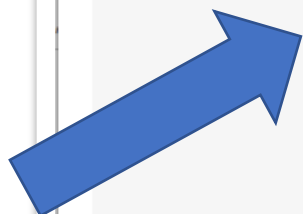
## SPEAR PHISHING

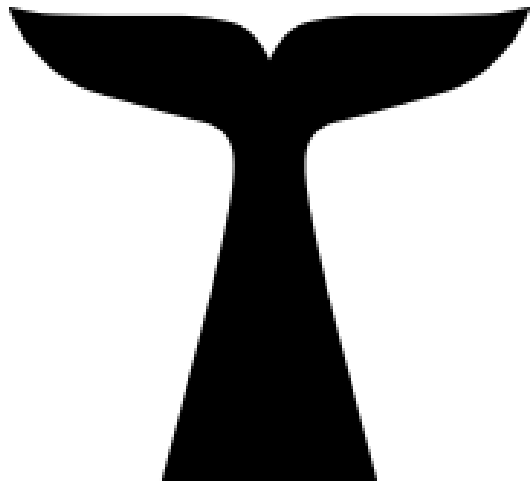
- Targeted
- Personal
- Harder to Detect





SPEAR  
PHISHING





## WHALING

- Email Spoofing Leaders in Organization
  - Superintendent
  - CEO
  - CFO
- Common Targets
  - Business Manager
  - Accounts Payable/Receivable
  - Secretary/Office Manager
- Very Convincing

----- Forwarded message -----

From: **Mwandle** <[Aaron882Smith@yahoo.jp](mailto:Aaron882Smith@yahoo.jp)>

Date: Thu, Sep 27, 2018 at 9:26 PM

Subject: bronco27

To: bronco27 <[mwandle@huntley.k12.mt.us](mailto:mwandle@huntley.k12.mt.us)>

I do know bronco27 is your passphrase. Lets get straight to point. You do not know me and you're probably thinking why you're getting this mail? Not a single person has compensated me to check you.

In fact, I placed a malware on the 18+ video clips (adult porn) website and you know what, you visited this site to experience fun (you know what I mean). When you were watching video clips, your web browser started out operating as a RDP having a key logger which provided me with accessibility to your display as well as webcam. Right after that, my software program collected all of your contacts from your Messenger, Facebook, and e-mail . And then I made a double video. First part displays the video you were watching (you've got a fine taste omg), and second part displays the recording of your web cam, and it is u.

There are 2 options. Why dont we read up on each one of these solutions in aspects:

First choice is to dismiss this e mail. In this scenario, I will send your very own video to almost all of your contacts and also just consider about the awkwardness yo u will see. Keep in mind should you be in an intimate relationship, just how it will certainly affect?

Number 2 alternative is to pay me \$3000. Lets call it a donation. Then, I most certainly will without delay delete your videotape. You will continue on your daily life like this never occurred and you would never hear back again from me.

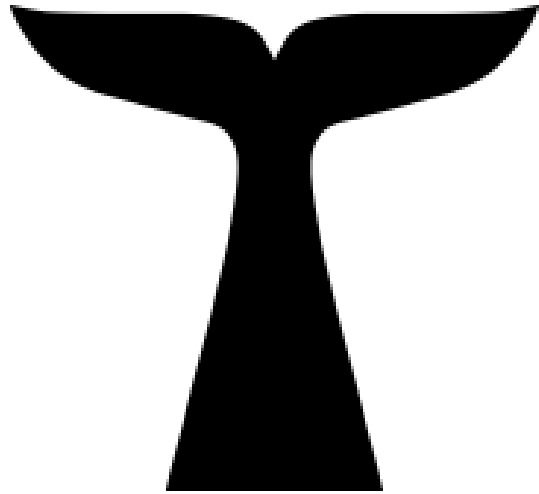
You'll make the payment through Bitcoin (if you don't know this, search "how to buy bitcoin" in Google).

BTC Address to send to: 1LagpngVjVB5bGNuNBdYUy98rS6oFV3Qhs

[case sensitive copy and paste it]

If you may be wondering about going to the law enforcement, very well, this message cannot be traced back to me. I have covered my actions. I am not attempting to charge a fee a whole lot, I want to be compensated.

You now have one day to pay. I have a unique pixel in this email, and now I know that you have read through this mail. If I don't get the BitCoins, I definitely will send out your video to all of your contacts including members of your family, coworkers, and so on. Nonetheless, if I receive the payment, I will destroy the video right away. If you really want proof, reply with Yes! then I definitely will send out your video recording to your 14 friends. This is the nonnegotiable offer, and so please don't waste my time and yours by responding to this e-mail.



WHALING

**From:** Superintendent Jane Doe [jane.doe@comcast.com](mailto:jane.doe@comcast.com)

**Sent:** Monday, January 30<sup>th</sup>, 2017 12:03 PM

**To:** Business Clerk John Smith

**Subject:** Important

Hello Sara,

Our auditor is requesting Social Security Numbers and Annual Payroll for all faculty. Please respond with information ASAP.

Thanks,

Jane Doe  
Superintendent

# Brute Force Attack



A brute force attack is one in which hackers try a large number of possible keyword or password combinations to gain unauthorized access to a system or file.



# Drive by Download

The infection of a computer with malware when a user visits a malicious website



# Drive by Download: Sources

- Malicious Websites
- Legitimate Compromised Websites
- Social Media Sites



# Distributed Denial of Services

An overload or shut down of services so that legitimate users can no longer access it. Most common target are web servers.



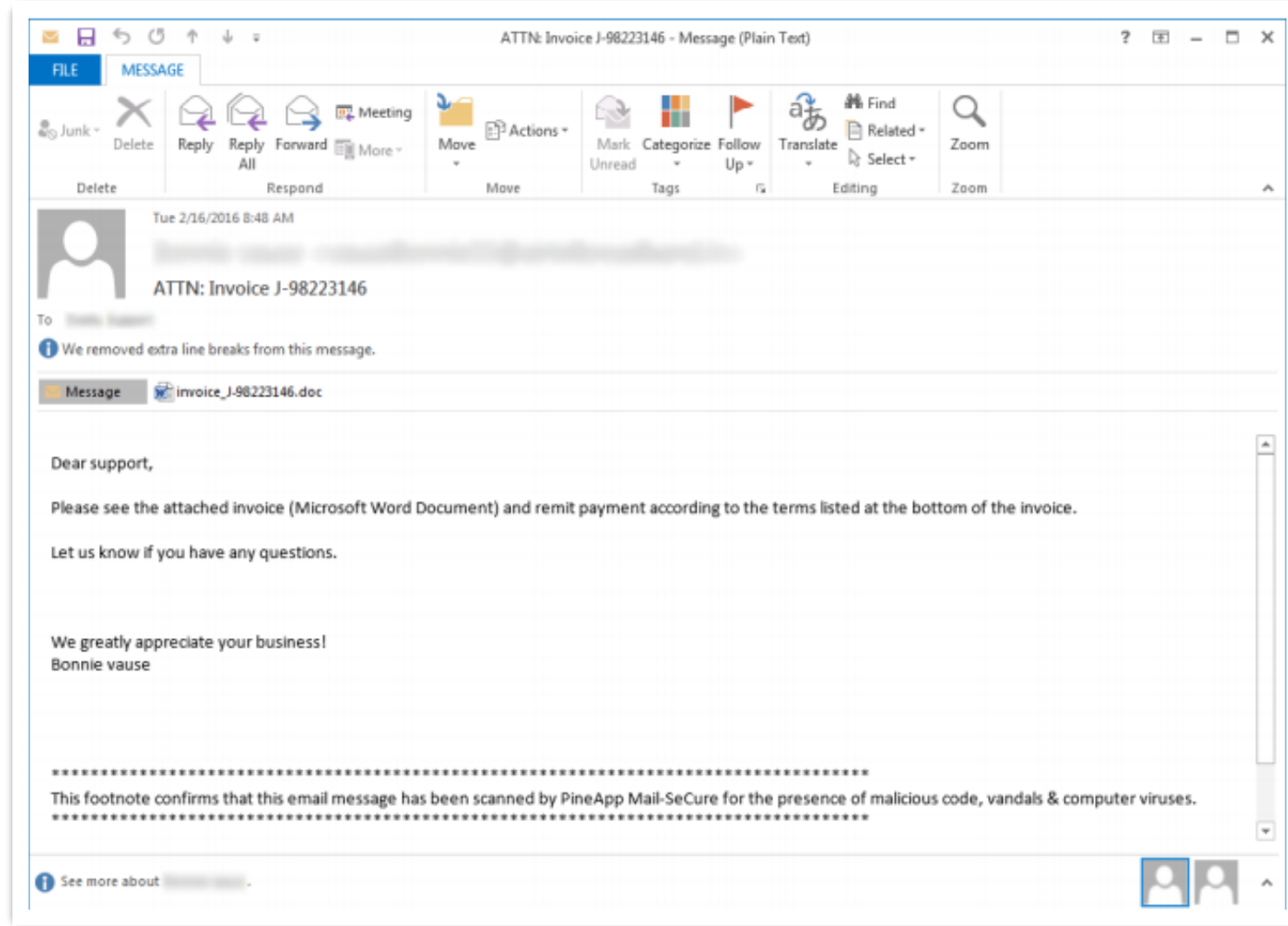
# Ransomware

Ransomware is software that denies you access to your files or computer until you pay a ransom

THE END OF  
RANSOMWARE

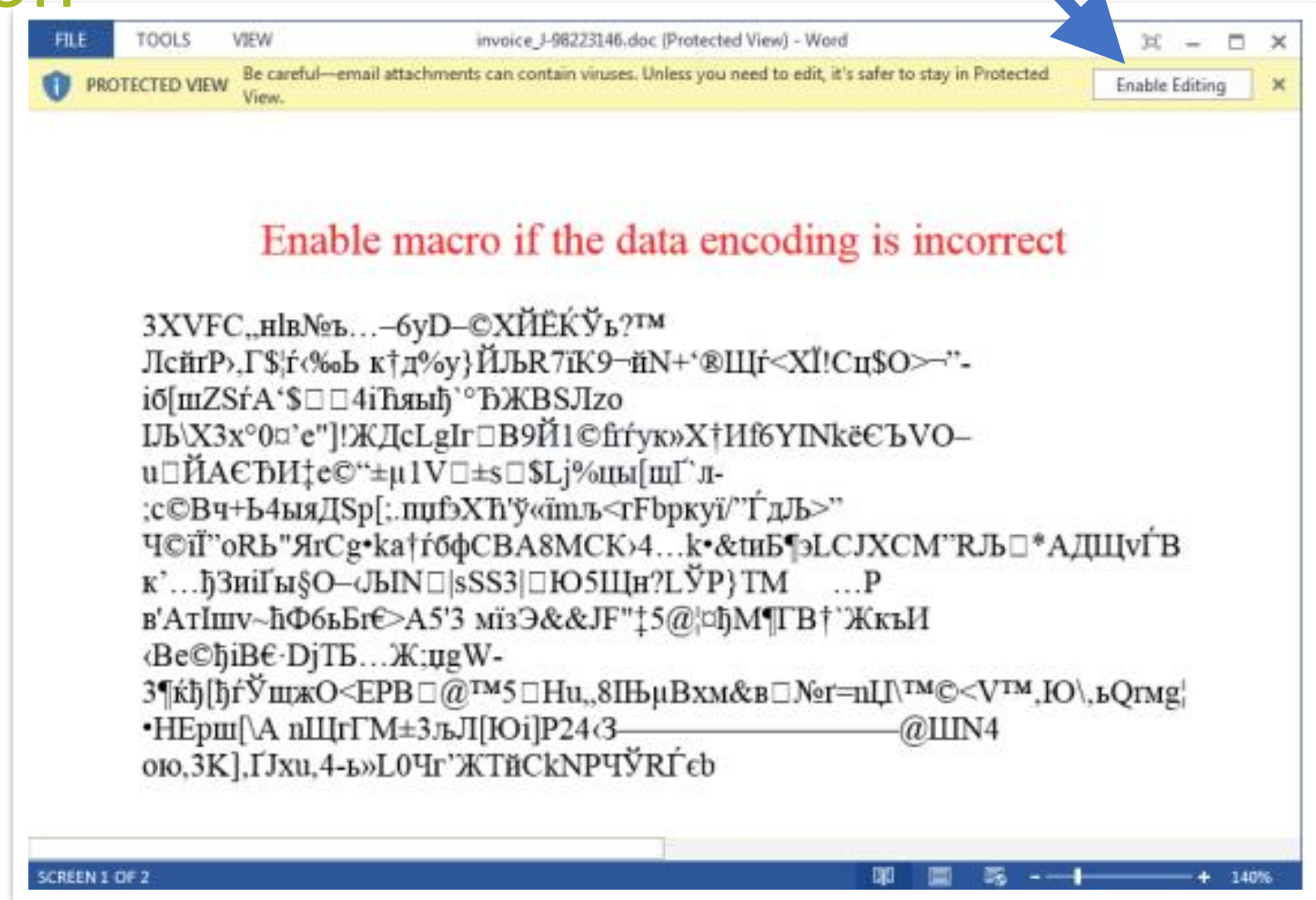
# Ransomware Example:

## Step 1: Advertisement of Exploit



# Ransomware Example:

## Step 2: Call to Action





# Ransomware Example:

## Step 3: Demand Ransom

**Your files are encrypted.**

To get the key to decrypt files you have to pay **500 USD**. If payment is not made before **20/07/15 - 19:41** the cost of decrypting files will increase **2 times** and will be **1000 USD/EUR**

Prior to increasing the amount left:  
**167h 56m 11s**

Your system: **Windows XP (x32)** First connect IP: **[REDACTED]** Total encrypted **330 files**.

[Refresh](#) [Payment](#) [FAQ](#) [Decrypt 1 file for FREE](#) [Support](#)

We give you the opportunity to decipher 1 file free of charge! You can make sure that the service really works and after payment for the CryptoWall program you can actually decrypt the files.

Your file is successfully decoded. You can download it

[Download decrypted file](#)

We are present a special software - CryptoWall Decrypter - which is allow to decrypt and return control to all your encrypted files.  
How to buy CryptoWall decrypter?

**bitcoin**

- You should register Bitcon wallet ([click here for more information with pictures](#))
- Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day.  
Here are our recommendations:
  - [LocalBitcoins.com \(WU\)](#) - Buy Bitcoins with Western Union
  - [CoinSafe.com](#) - Recommended for fast, simple service. Payment Methods: Western Union, Bank of America, Cash by FedEx, Moneygram, Money Order. In NYC: Bitcoin ATM, In Person
  - [LocalBitcoins.com](#) - Service allows you to search for people in your community willing to sell bitcoins to you directly.
  - [btodirect.eu](#) - THE BEST FOR EUROPE
  - [coinmr.com](#) - Another fast way to buy bitcoins
  - [bitquick.co](#) - Buy Bitcoins Instantly for Cash
  - [How To Buy Bitcoins](#) - An international directory of bitcoin exchanges.
  - [Cash Into Coins](#) - Bitcoin for cash.
  - [CoinJar](#) - CoinJar allows direct bitcoin purchases on their site.
  - [anxpro.com](#)
  - [bittylicious.com](#)
  - [ZipZap](#) - ZipZap is a global cash payment network enabling consumers to pay for digital currency.
- Send **1.79 BTC** to Bitcoin address: **[REDACTED]**
- Enter the Transaction ID and select amount:  
 **1.79 BTC ≈ 500 USD** [Clear](#)  
Note: Transaction ID - you can find in detailed info about transaction you made.  
(example 44214efca50ef039388db929e40bf34f19a27042f07f5cf3e2aa08114c4d1f2)
- Please check the payment information and click "PAY".

[PAY](#)

# Why it matters to **YOU**

On average it take **640 hours** to restore your identity if you're the victim of identity crime.

**YOU** are the target, criminals want what you have.

Being cyber safe helps protect those **you care about**.

A child is **51% more likely** to be the victim of an identity crime then their parents

# Final Tips

## Create good passwords

- Simple, long and memorable
- Try personal sentences, then add in numbers and special characters
- Test your password –  
<http://www.passwordmeter.com>

## Avoiding Phishing Schemes

- Take a quiz –  
<https://www.sonicwall.com/phishing/>

## Run Updates

- Restart your computer

## Lock your computer screen



mbranger@huntley.k12.mt.us