Cybersecurity for Law Firms

by Marco Alcala

marco@alcalaconsulting.com

310-984-7007

Agenda

Business Email Compromise Attacks

Ransomware Attacks

Questions and Answers

What are business email compromise attacks?

Examples of Business Email Compromise Attacks

CEO Fraud

Fake Invoice Scheme

INVOICE #	12491
INVOICE DATE:	02/01/2024

mith, and Jon

093 25th St,
ort Arthur, Texas 77642
hone: 210-555-1122
@smithjones.law
ww.smithjones.law

BILL TO
Accounts Payable
304 Almquist St
254-555-2345
ap@abcmanufacturing.com
Customer ID: 0491133

QTY	ITEM ID#	DESCRIPTION	UNIT PRICE	ITEM TOTAL
1		Account Recovery	$65,000.00	$65,0

SUBTOTAL	$65,

PAYMENT TERMS	
PAYMENT DUE	

TAX	
TOTAL DUE	$65,

Make All Checks Payable To: Smith, and Jones Law

THANK YOU FOR YOUR BUSINESS!

Email Account Compromise

Attorney Impersonation

Data Theft

Change of Bank Account Details

How to Protect Against BEC Attacks

Employee Training and Awareness

SENDER POLICY
FRAMEWORK (SPF)

DOMAINKEYS IDENTIFIED
EMAIL (DKIM)

DOMAIN-BASED MESSAGE
AUTHENTICATION (DMARC)

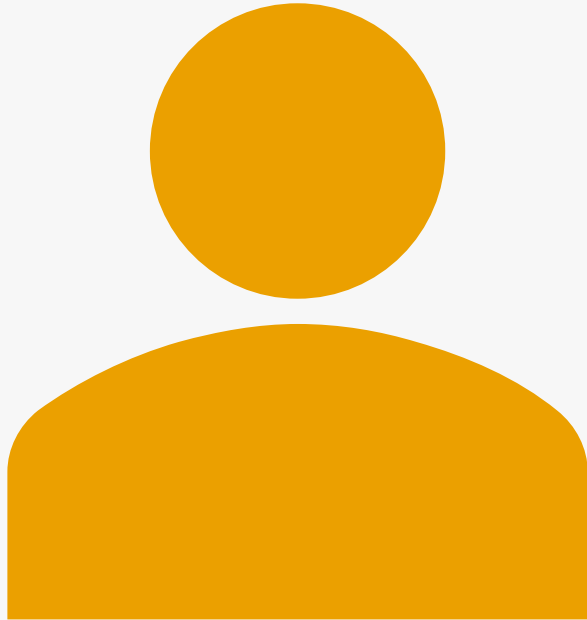# Email Authentication Protocols

Advanced Email Filtering

Multifactor Authentication

Verification Procedures

Access Controls and Segmentation
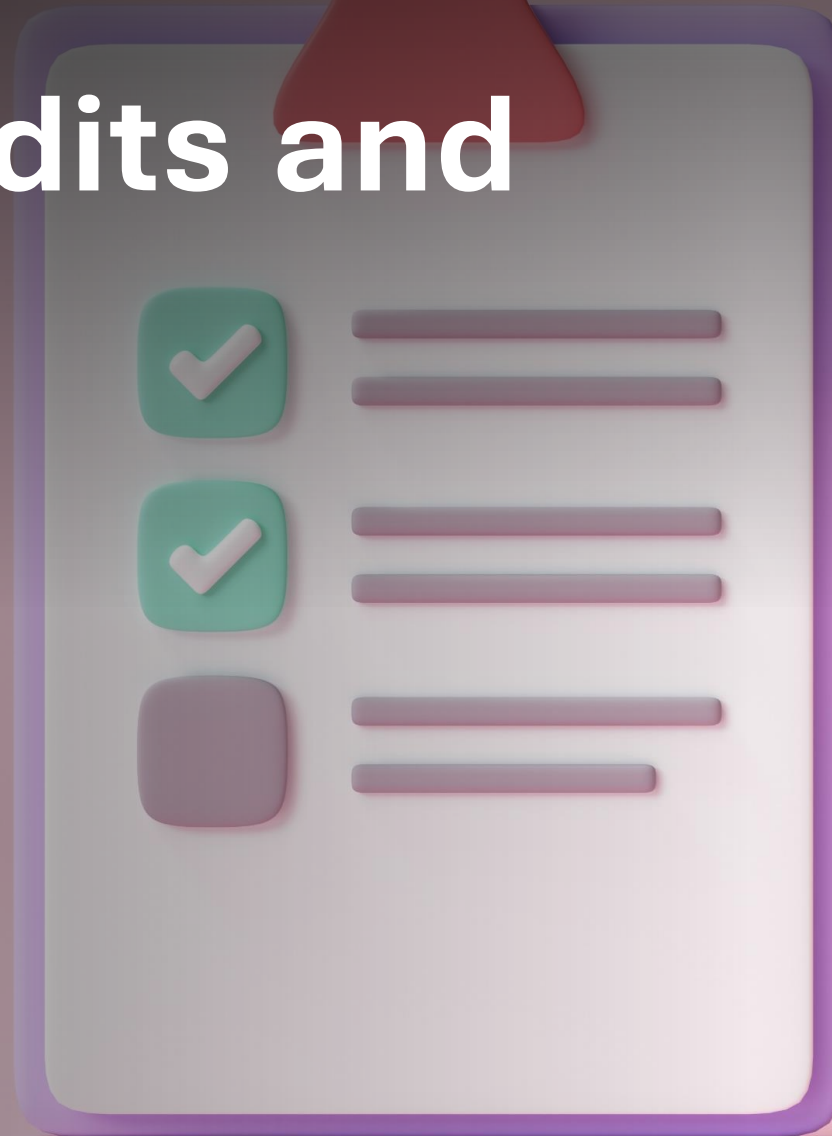
Regularly Update and Patch Systems

Out-of-Band
Communications

Incident Response Plan

Regular Audits and Reviews

What is a Ransomware Attack?

CryptoLocker

Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key.**

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **300 USD / 300 EUR /** similar amount in another currency.

Click «Next» to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Private key will be destroyed on
10/9/2013
4:25 PM

Time left

Regular Data Backups

Update and Patch Systems

Compliance Security Stack

2FA/MFA

Email Security

Security Awareness Training

Phishing Simulation

Anti-Phishing Platform

Password Vault

Application Control

All the time VPN for remote computers

Web Gateway Security

Ring-Fencing

Computer Encryption

Security Information and Event Management (SIEM)

Managed Detection and Response (MDR)

Security Operations Center (SOC)

Incident Response Plan

Questions and Answers

Thank You