aasbo | Alabama Association of School Business Officials

Digital Security

Susan Poling, Executive Director

ALET ALABAMA LEADERS *in* EDUCATIONAL TECHNOLOGY

May 2022

Cyber Security

This Photo by Unknown Author is licensed under CC BY

Prevention of *damage to*, protection of, and restoration of *computers, electronic communications systems, electronic communications services*, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

https://www.secureworld.io/industry-news/cybersecurity-vs-data-security-definition

Data Security

Data Security concerns the *protection of data* from accidental or intentional but unauthorized modification, destruction or disclosure through the use of physical security, administrative controls, logical controls, and other safeguards to limit accessibility.

https://www.secureworld.io/industry-news/cybersecurity-vs-data-security-definition

Schools are Preferred Targets for Both Types of Crime Because . . .

- Valuable data
- Technology-dependent
- Large bank accounts
- Connections to community
- Small IT and security budgets

Cybercrime Won’t Stop

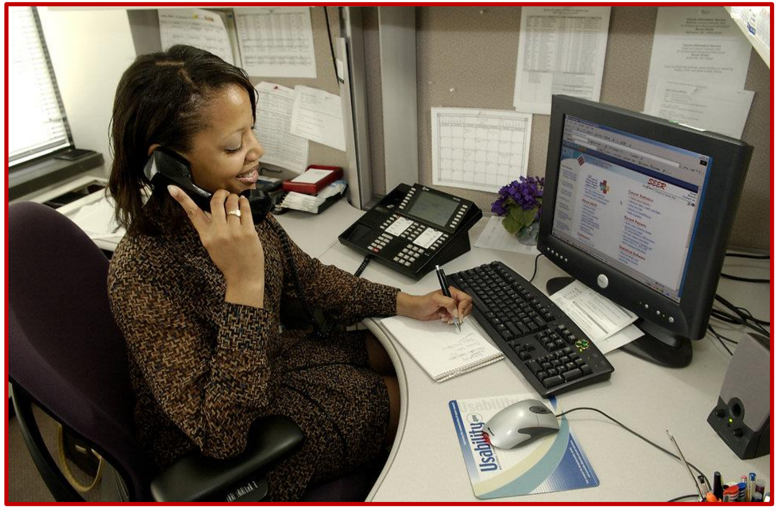
- Can do it from anywhere in the world
- Does not take a high level of technical skill
- Some do it for extra income or as their main ‘job’
- Cyber gangs and nation states participate
- Many crimes go unreported to law enforcement
- Harder to get caught
- Non-violent crime so punishments are less

https://www.educba.com/cyber-crime-in-india/

Accounting Staff

Because you can access personal data and bank accounts

YOU are a **high value target** **within a** **high value target.**



Technology Department

Digital security is a shared responsibility.

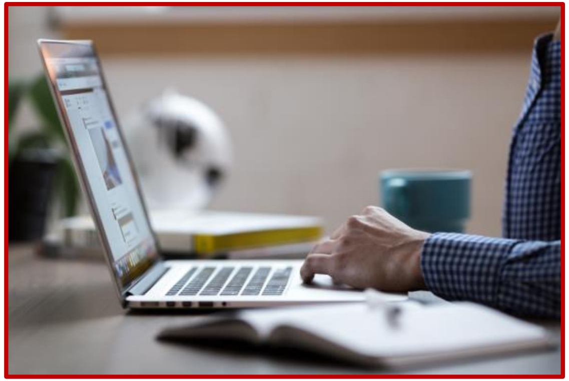
The IT Department cannot do it alone.

This Photo by Unknown Author is licensed under CC BY

Accounting Staff

Detect, Defend, & Respond

1. Recognize techniques used by cybercriminals.
2. Learn how to prevent exposing data.
3. Apply best practices diligently.
4. Report suspicious incidents immediately.



Accounting-Related Cyber Crimes

- Identity Theft
- W-2 Theft
- Direct Deposit Theft
- Gift Card Scams
- Purchase Order Scams

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

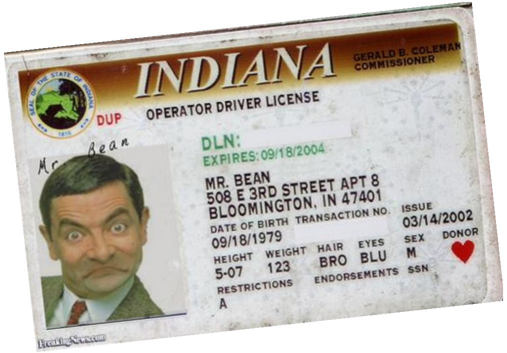
Personal Identifiable Information (PII)

- Social Security Numbers
- Date of Birth
- Driver’s License
- Address
- Phone Numbers
- Email Addresses

Some can be used alone, but others need to be combined to in order to be useful to criminals.

Identity Theft Uses

- File fake tax returns
- Open bank accounts
- Open credit card accounts
- Get a driver’s license
- Take out loans
- File medical claims against your health insurance policy
- Commit criminal acts that go on record for you
- Make fraudulent insurance claims
- Get hired using you for the background check



INDIANA
GERALD B. COLEMAN
COMMISSIONER
SEAL OF THE STATE OF INDIANA 1816
DUP
OPERATOR DRIVER LICENSE
Mr. Bean
DLN:
EXPIRES: 09/18/2004
MR. BEAN
508 E 3RD STREET APT 8
BLOOMINGTON, IN 47401
DATE OF BIRTH 09/18/1979
TRANSACTION NO.
ISSUE 03/14/2002
HEIGHT 5-07
WEIGHT 123
HAIR BRO
EYES BLU
SEX M
DONOR ♥
ENDORSEMENTS
SSN
RESTRICTIONS A
FreakingNews.com

EXPOSING DATA BY DOWNLOADING FILES

Don’t download files with PII to:

- Any personal device
- A work computer that is not assigned to you
- An unsecured laptop or tablet that is assigned to you

System-owned laptops used by accounting staff should be fully encrypted with a program such as Windows BitLocker*. If the device is lost or stolen, the data on it won’t be accessible.

*Talk to IT Director about securing/encrypting laptops. Do not try to install yourself.

Delete Downloaded/Cloud-Saved Files

Computer/OneDrive/Portable Media (USB, etc.)

- Delete the files
- Empty trash or recycle bin

Google Drive

- Right-click, Remove
- Trash, Select file, Right-click, Delete forever

W-2 THEFT

Often comes in the form of a *fake* or *compromised* email from a high-ranking employee.
(Superintendent, CSFO, etc.)

From: CSFO
To: You
Subject: Need Info

Kindly send me the individual 2021 W-2 (PDF) and earnings summary of all W-2 of our staff for a quick review.

NEVER reply to these emails. Call the person on the phone or see them personally.

If the request is legitimate, don't use email to transmit the information.

If fake, report the email to the IT Department.

IRS directions for reporting W-2 phishing emails can be found at

https://www.irs.gov/individuals/form-w2-ssn-data-theft-information-for-businesses-and-payroll-service-providers

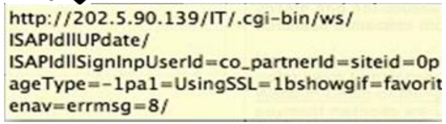
Hover your pointer over the sender’s name to see the actual email address.

From: Fred Watson

Fred.Watson@shelby.it.org

Subject: URGENT!

Your email is almost full! You must reauthorize your account in order for to continue using. Click here to reset your account.



```
http://202.5.90.139/IT/.cgi-bin/ws/
ISAPIdllUPdate/
ISAPIdllSignInpUserId=co_partnerId=siteid=0p
ageType=-1pa1=UsingSSL=1bshowgif=favorit
enav=errmsg=8/
```

IT Supervisor

Look for familiar links with wrong first/last name format or *extra* parts in the URL, such as www.shelbyed.it.org

Links could take you to a website that downloads malware in the background that scrapes passwords saved to your browser.

Fake Online Password Reset Page

This is what they want.

Reset Your Account

Email:

Login ID:

Current Password:

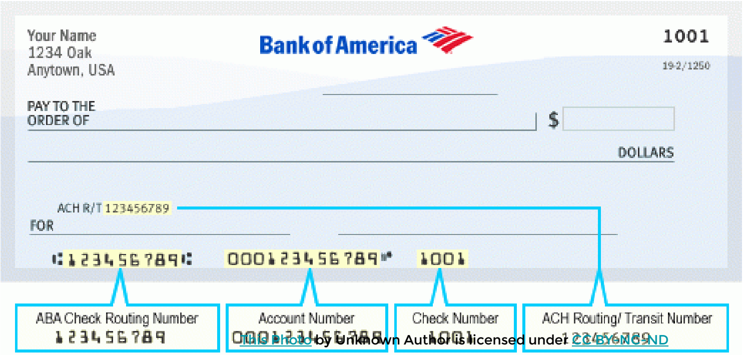
New Password*:

Confirm Password:

*Must be at least 8 characters and contain at least one capital letter, one lower case letter, a number and a special character !#$()-

ROUTING NUMBER SCAMS

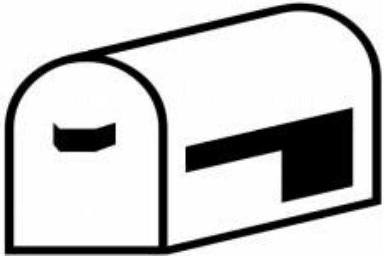
- Payroll direct deposit
- Accounts payable

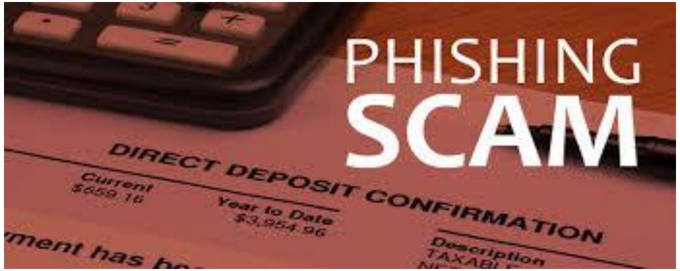


This Photo by Unknown Author is licensed under CC BY-NC-ND

PAYROLL DIRECT DEPOSIT SCAM

The FBI has been warning colleges and schools about direct deposit payroll scams since 2017.





About the same time many employers switched from paper checks to automatic deposit. This change has made it so much easier for thieves.

Payroll Direct Deposit Scam

Direct Deposit scams often begin with:

- Fake emails that attempt to get key information from either the payroll staff or the employee.

- Stealing login and password information for payroll or ESS software.

FAKE, from fake account.

From: HR Services
Subject: Email Change Alert

This email is to confirm that you have successfully updated your email via Self Service portal.

The update occurred on 5/1/0222 at 10:53 a.m.

If you did not update this information online, please go to eid/help/stolen.html or call the helpdesk for assistance.

Please note that if you have multiple email accounts with us, you may receive this message at each email address.

Changing the Routing Number

From: Suzan Poling
To: Vera Jones
Subject: Direct Deposit Change

FAKE, but from actual account.

Vera,
I'm changing banks and need to change where my paycheck is deposited as soon as possible. My Regions account is going to be closed this weekend, so please make the change to my new account at PNC before payday. Info below:

PNC 043002900 888 2421 5

Thanks

Once the criminals have the information, they will either -

1. Contact the payroll department, convince the clerk that they are the employee by using the stolen information, and have the clerk change the routing number, or

2. Log into the payroll or ESS software and change the routing number.

Account Closed

As soon as the ‘paycheck’ is deposited, the criminals use ATMs or debit cards to empty the bank account they have set up. Then they close the account or abandon it.

Accounts set up with stolen IDs to start with.

$0 Payday

Once the employee realizes their salary was not deposited, they will be calling the payroll department.

Impact on System & Employee

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

School systems lose money if they double-pay the employee.

For employees who autopay bills at the start of the month, this can lead to insufficient to cover their bills.

Onboarding Should Include Cybersecurity Training

- All employees need cyber training plus specific info about direct deposit scams.
- Payroll staff should get specific training on digital security practices and procedures.

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

Implement & Advertise System Policies

○ IT, HR, and Payroll will never send emails with links prompting password changes or requests for personal information.

○ Warn employees not to access ESS systems from insecure networks or devices.

Protective Measures

1. Don’t allow employees to change their own routing numbers.
2. Don’t allow spouses to request changes to routing numbers.
3. Require verification of all change requests, such as –

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

- ○ Employee must personally come to the office and provide ID if not personally known to payroll staff.
- ○ All requests submitted by phone, fax, or email must be validated by the employee’s supervisor.
- ○ Payroll staff should log the request and the verification method.

ACCOUNTS PAYABLE SCAMS

Criminals will use your website to –

- Identify the companies you do business with
- Use that company's website to create fake emails, spoof phone numbers, impersonate company staff over the phone, etc. to request or send a routing number change.

- Payments start being deposited into the wrong bank accounts.
- It may take months before a company reports not being paid.

(SHREVEPORT, LA) - **Almost $1 million in public funds, designated for a charter school in Shreveport, were diverted from a Caddo Parish school system account to an overseas account** as part of a cyber crime, officials acknowledged on Tuesday. Financial crimes detectives and Caddo Parish school system officials described it as a phishing scheme.

They were phished through an account based in Africa, officials said.

That scammer "spoofed an official charter email account to change banking information on file with Caddo Schools," the Caddo Parish school system said in a statement Tuesday morning. "As a Type 1 charter, the district makes payments to Charter Schools USA based on Magnolia School of Excellence’s enrollment. "

Pay by Check for Extra Security

The first payment after a routing number change should be paid by check.

If the employee or company didn’t request the change, the paper check will alert them, and they will probably call payroll/accounting to find out why.

Not seeing the automatic deposit would alert them too, but this way no funds are lost.

PURCHASE ORDER SCAM

- Criminal uses your logo to create a fake PO
- Fakes an email or fax number from your system
- Sends the PO to a vendor from the fake fax or compromised email
- Has the equipment delivered to an alternate address
- Collects the equipment and then sells it
- System gets the invoice for materials it never ordered

This Photo by Unknown Author is licensed under CC BY

GIFT CARD SCAM

- Receive a fake email impersonating a supervisor or fellow staff member
- Instructed to purchase gift cards to use for some school function
- Instructed to send gift card information via email to the ‘supervisor’
- Victim uses their own money thinking they will be reimbursed or uses a System credit/debit card
- Criminal sells or cashes in the gift cards

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

INSECURE WI-FI

Never consider open Wi-Fi to be safe. This includes:

- Airports
- Restaurants and Stores
- Hospitals
- Hotels

3 Public WiFi Risks
1. Packet Sniffing
2. Man-in-the-Middle Attacks
3. Malicious WiFi Hotspots

Source: https://rmonnetworks.com/public-wifi-risks-and-how-you-can-avoid-them/

Malicious Wi-Fi Hotspots

- Criminal sets their device up as a hotspot with a name that you won't suspect is not the official 'free' Wi-Fi.
- While you browse, email, etc. your traffic is recorded and later analyzed for any useful information.

Source: https://rmonnetworks.com/public-wifi-risks-and-how-you-can-avoid-them/

Packet Sniffing on Public Wi-Fi

- The IT equivalent of wire tapping
- Can capture sites you are visiting including your login id and password
- With certain software they can also capture your key stokes so encryption does not completely protect you

Source: https://rmonnetworks.com/public-wifi-risks-and-how-you-can-avoid-them/

VPN – Virtual Private Network

Do NOT use personal devices for your accounting work. However, if you want to add some protection for your personal use of your personal devices, you may want to purchase a VPN product. They cannot guarantee you can't be compromised on public Wi-Fi but add a layer of protection for you by encrypting your traffic. Some websites such as Netflix, etc. don't allow access if your VPN is activated.

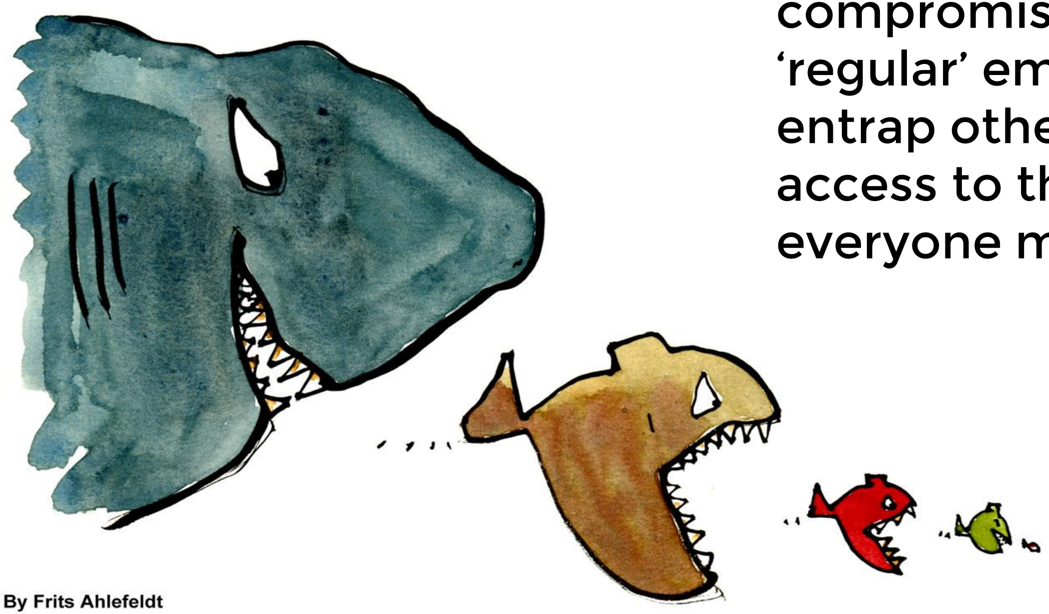
Do NOT choose a Free VPN client

- Collect & sell customer data
- Inject advertising
- Collect location data
- May have lower encryption

Look for Highly-Rated VPN Apps

- PrivateInternetAccess
- ExpressVPN
- CyberGhost
- $3.00 to $7.00 per month
- Covers multiple devices
- Can run on mobile devices, including your phone.
- Check reviews before purchasing

Any Compromised Account . . .



By Frits Ahlefeldt

Criminals may use the compromised email accounts of ‘regular’ employees in order to entrap others with higher-level access to the data they want. So, everyone must be on their guard.

Procedures and Safeguards

- Don’t publish names and emails of AP or Payroll staff online.

- Limit the number of individuals who can change routing numbers.

- Use strong passwords that are changed frequently.

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

ACCOUNTING SECURITY PRACTICES

- Prohibit risky email practices
  - Don’t use district email address for personal use
  - Don’t check personal email on district devices
- Expect off-campus use of devices/accounts to be safe
  - Prohibit accessing critical accounts over public Wi-Fi
  - Prohibit downloading of senstive data to personal equipment
- Require Multi-Factor-Authentication for high risk accounts
- Prohibit employees from saving passwords in browsers at work and at home

All accounting staff should be considered ‘high risk’ accounts.

ACCOUNTING SECURITY PRACTICES

- Review logs routinely for unusual activity
  - Unusual login times
  - Unusual IP address connections

https://www.educba.com/cyber-crime-in-india/

- Review all routing number changes shortly before payroll or accounts payable schedules

- Work with the IT Dept. to scan for unusual email access times or originating IP addresses

Detect, Defend, Respond

Accounting staff have a higher duty of care.

Keep your training up-to-date and ALWAYS apply safe practices.

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

Thank You

ALET

ALABAMA LEADERS in EDUCATIONAL TECHNOLOGY