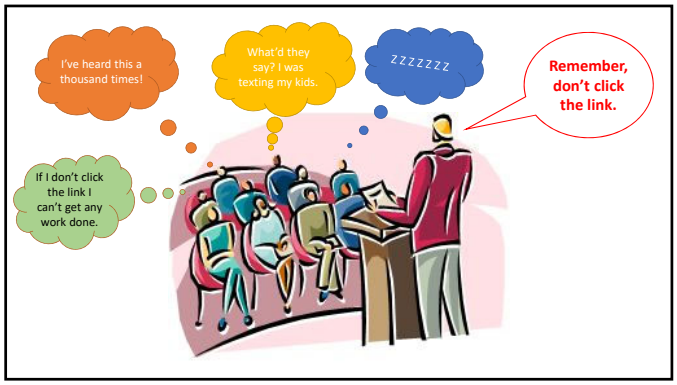
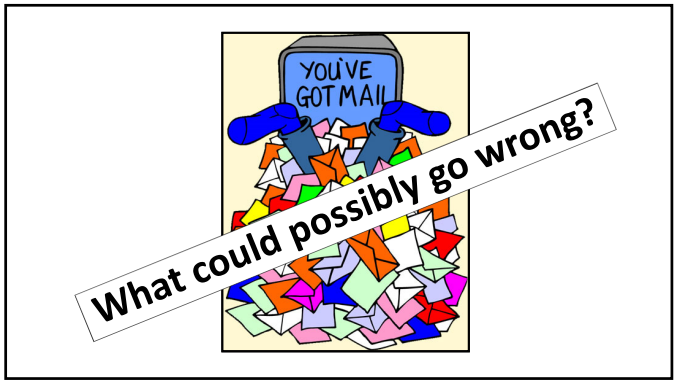
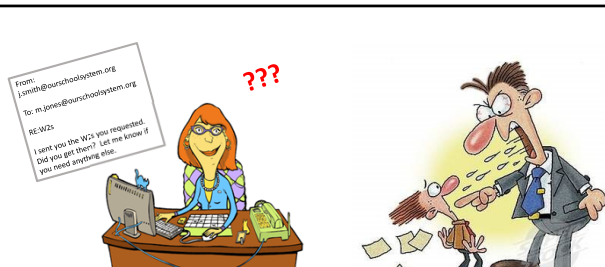
ALABAMA LEADERS in EDUCATIONAL TECHNOLOGY

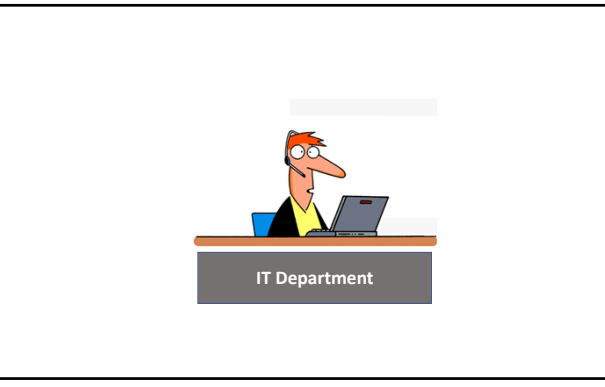
Susan Poling, Executive Director





From: Superintendent Jones
To: j.smith@ourschoolsystem.org
RE: Report Needed
We have been asked to report all W-2 filings to the State. Please email our annual W-2 as an attachment as soon as you can get to it. I need this by noon.


From:
j.smith@ourschoolsystem.org
To: m.jones@ourschoolsystem.org
RE:W2s
I sent you the W2s you requested. Did you get them? Let me know if you need anything else.
???


IT Department

- The tech department cannot stop the inflow of email.
- We can't afford services that check the security of links and documents contained in every incoming email.
- **Even if they could, this wouldn't protect us 100%.**

Date Made Public:	April 22, 2016
Company:	Berkeley Public Schools
Location:	Berkeley, California
Type of breach:	DISC
Type of organization:	EDU
Records Breached:	0

The Bay Area News Group, a publisher of multiple Bay Area newspapers, requested information on

The employee who transmitted the information to the news group inadvertently put Social Security numbers of the employees as part of the information.

More Information: http://oag.ca.gov/ecrime/databreach/reports/sb24-61243

Information Source: California Attorney General

Medical records of high school students leaked in 'appalling' data breach

Medication, healthcare records, and conditions were all posted online for the world to see.

By Charlie Osborne for Zero Day | August 23, 2018 -- 09:49 GMT (02:49 PDT) | Topic: Security

A data breach has taken place at a Melbourne high school which healthcare records of students being published online.

The security incident, which took place at Strathmore secondary college in Melbourne, was deemed "nothing short of appalling" by Victoria education minister, James Merlino, as reported by The Guardian.

In total, over 300 records were reportedly published online late Monday evening and remained available until Tuesday. The records included data on student physical and mental health conditions, medications required, as well as behavioral and learning difficulties.

"It's distressing for students and their parents because it may result in embarrassment, in bullying," Merlino said. "These things should not happen."

Human error was believed to be the cause of the publication of more than 300 students' records on the school's intranet service which, according to News Corp reports, included information about medical and mental health conditions, medications, and learning and behavioural difficulties.

If you have access to confidential data, you are always just one click away from making a serious mistake.

When!
Not If.

Hacker obtains or creates a believable PDF file and embeds executable malware in it.

Sends phishing email to a specific target or broadcasts to many potential victims.

Employee opens PDF file, releasing malware

Malware overwrites executable programs that the computer uses to run with new instructions.

Malware gives hacker access to systems.

Hacker controls, steals data, or uses computing power to attack other systems (DNS) until discovered.

Profiting from Stolen Credit Cards

- Sell credit/debit cards online, but not very profitable
- Use card to buy expensive products like iPhones that they can then sell
- Use card to buy gift cards that they can sell online at a discount

Profiting from Stolen Credit Cards

- Recruit or become an Uber (Lyft, etc.) driver
- Book fake trips using stolen credit/debit card
- Driver gets paid
- Driver splits fare with hacker

Profiting from Account Access

Log into the account and order products.

If a debit card is the stored method of payment, the victim might find their bank account empty.

Profiting from Bank Account Access

- Hackers use phishing emails to trick employees into giving them their payroll portal login credentials OR enough information about the employee to impersonate the employee
- They open a bank account
- Change the routing of the direct deposit to their bank account
- Employee gets paid
- Hacker empties bank account via debit card or simply withdrawing all the funds

It's Not All Criminal Gangs

- About 15% use revenues to pay their mortgages and their bills.
- Others, . . . who were making a lot of money, . . . got involved in "old-fashioned ostentatious spending."
- A lot of them are converting their money to assets and investing in them to acquire status.

Source: BBC News - https://www.bbc.com/news/technology-44355153

Bank Account Swapping on a Larger Scale

(SHREVEPORT, LA) - **Almost $1 million in public funds, designated for a charter school in Shreveport, were diverted from a Caddo Parish [illegible] account to an overseas account**

Threats can come from anywhere.

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. "

Identity Theft

Specific information:

- Full name
- Address
- Social Security number
- PIN codes and passwords
- Financial account numbers

Other, less accessible items may include:

- Personal information (for answering security questions) like your favorite food, book, or mother's maiden name
- Birth certificates or passports
- Old copies of credit reports and financial statements

Source: https://www.myidcare.com/about-id-theft

Identity Theft Uses

- Opening bank accounts
- Opening credit card accounts
- Taking out loans
- Filing medical claims against your health insurance policy
- Committing criminal acts that go on record for you
- Getting hired using you for the background check
- Getting a driver's license
- Making fraudulent insurance claims

Children's Identity Theft

Provides a blank slate:

- No credit checks
- No credit history
- No driver's license
- No debt

They won't find out until years later.

The average age of a child whose identity is stolen is 12 years old.

TOPICS SEARCH **Los Angeles Times**

San Diego Unified data breach hits staff, plus as many as 500,000 students

By KRISTEN TAKETA | DEC 21, 2018 | 3:10 PM | SAN DIEGO

The personal information of San Diego Unified students, former students and employees may have been compromised in a data breach that officials believe happened in January, the school district said Friday.

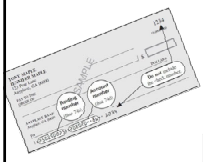
The breach could affect as many as 500,000 students who attended San Diego Unified schools as far back as the 2008-09 school year, officials said.

The breach may have included information about students and staff such as addresses and dates of birth, discipline, health, scheduling and grade information, according to an email sent to school families on Friday. Social Security numbers were also affected.

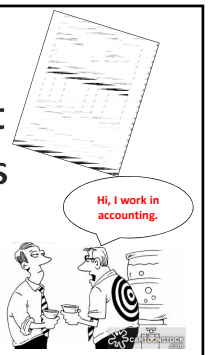
More than 50 employees clicked the link in the infected email, giving the hacker access to the Student Information System containing the Social Security numbers of past and present students.

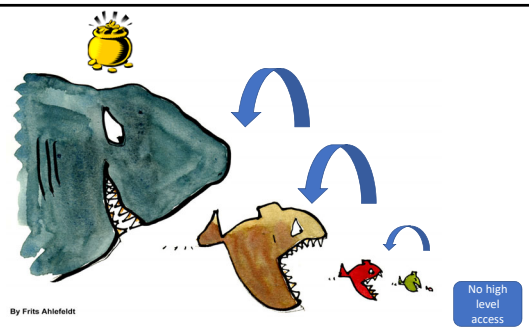
Higher Duty of Care

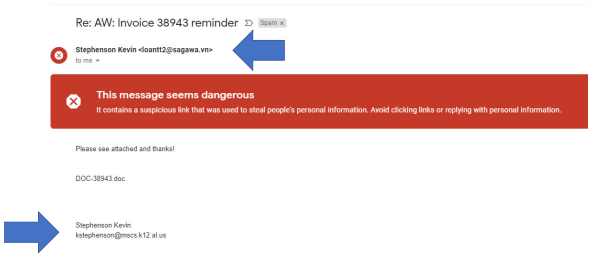
Position	Reason
Technology director and network staff	Passwords and access to all servers and most applications Ability to create accounts and grant rights to others Authority figure whose directions people will follow
Superintendent, Supervisors, Administrators	High level data access Authority figure whose directions people will follow
Accounting Staff – all levels	Access to payroll, banking, and accounts payable
Registrars/Counselors – INOW	Passwords and access to Student and Employee information Registrars – Ability to create accounts and grant rights to others
Nurses	Access to confidential health data records



Identity Theft
Direct Deposit
Bank Transfers
PO Fakes
W-2 Theft







---------- Forwarded message ----------
From: James McCoy <debengsth@gmail.com>
To:
Cc:
Bcc:
Date: Wed, 5 Dec 2018 15:34:30 +0000
Subject: LETTER FROM THE SUPERINTENDENT Dr. JAMES McCOY
Dear Colleagues:

Due to our continued commitment to fostering an environment that is safe and secure, inclusive, and conducive to academic inquiry, student engagement and student success. Whether it's improving safety and reliability, delivering better service for our students, or earning back their trust and confidence, all of us at this institution are working hard to ensure that our organization is on a solid foundation for the future.

This Policy applies to all employees, as it aims to provide guidance and align our behaviors as we make great decisions that impact our daily operations. we rely on our values and this code as guidelines, as a breach of the Policy may result in disciplinary action against the Employee concerned.

All employees, including all individuals on full-time or part-time employment with the Institution are required to go through the guidelines attached in this email. It is important that we all adhere to these guidelines so you will be helping to ensure a future success of this great institution

Thank you for your ongoing commitment to delivering a better and reliable service.

Sincerely,

Dr. James McCoy
Superintendent

Don't Help the Hackers

Posting the job titles and email address of accounting staff on **public** websites just makes the hacker's job easier.

Our Wonderful Website	
Accounting Department	**Email**
John Doe, CSFO	jdoe@xyz.org
Jane Smith, Chief Payroll Clerk	j3smith@xyz.org
Dan Brown, Accounts Payable	d8brown@xyz.org

From: Jan@excel1.com
To: d8brown@xyz.org
Subject: Free Excel Tips and Tricks

Save yourself hours every week using these quick tips. This is a free offer being sent to accounting staff of public school systems. Click the PDF to learn how to save yourself hundreds of hours of work every year.

Never Update Login Credentials from a Link

Once they get your current password they will log in as you and do whatever they want.

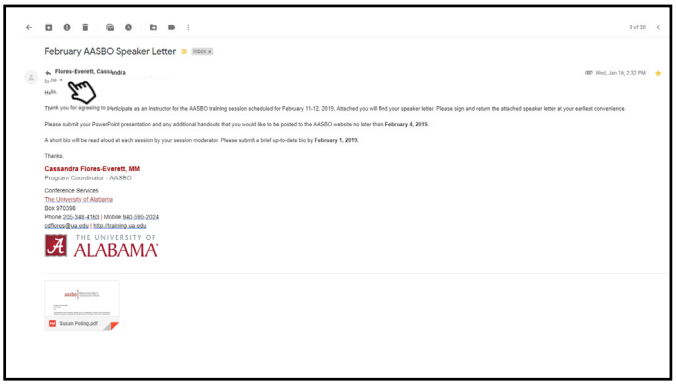
ANYONE can create a form like this and post it to a fake website that they also create.

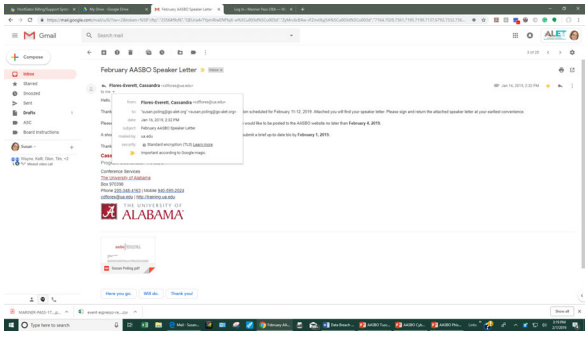
READ!

Never click on a link or an attachment until you read the email and check out who sent it.

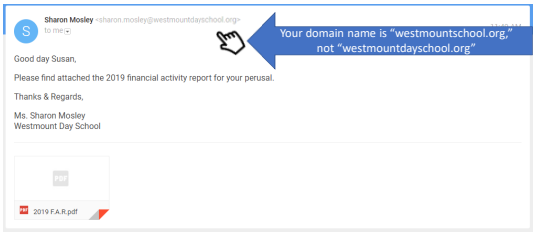
Quit Skimming – Change Your Bad Habits

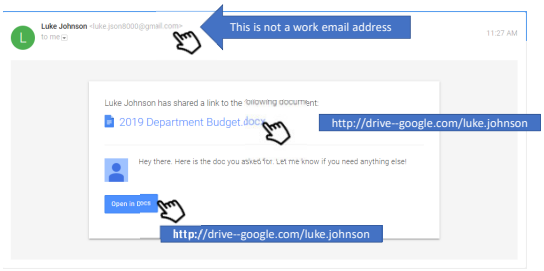
- Don't open more than a few emails in one session.
- Come back to an email later if you are tired or rushed.
- Always check Sender email address.
- If the email asks for any critical data, phone someone to verify the request is legitimate.

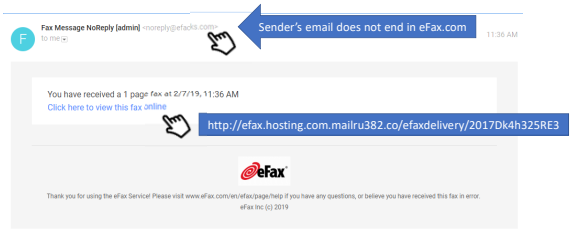


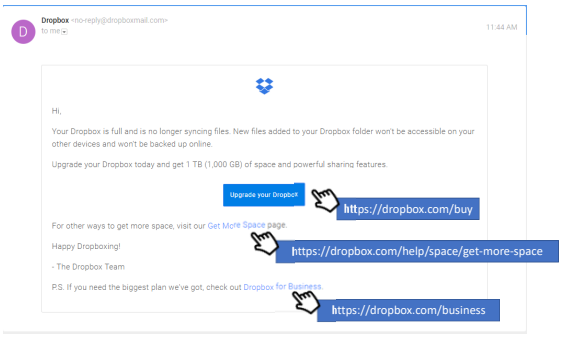


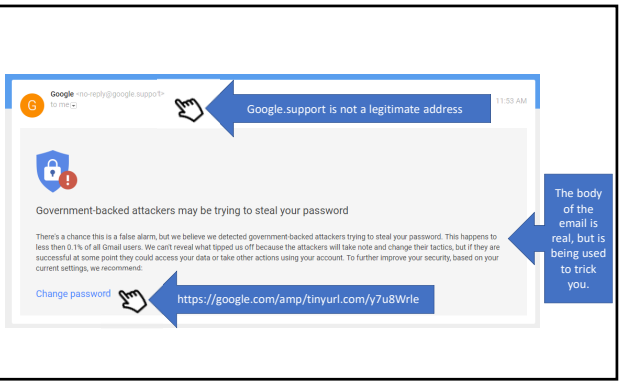
Know Your Domain Addresses



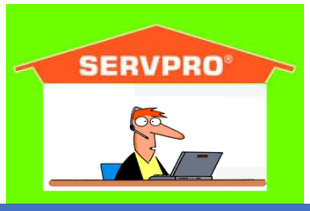





Dropbox <no-reply@dropboxmail.com>
to me
11:44 AM
Hi,
Your Dropbox is full and is no longer syncing files. New files added to your Dropbox folder won't be accessible on your other devices and won't be backed up online.
Upgrade your Dropbox today and get 1 TB (1,000 GB) of space and powerful sharing features.
Upgrade your Dropbox
https://dropbox.com/buy
For other ways to get more space, visit our Get More Space page.
https://dropbox.com/help/space/get-more-space
Happy Dropboxing!
- The Dropbox Team
P.S. If you need the biggest plan we've got, check out Dropbox for Business.
https://dropbox.com/business


Google <no-reply@google.support>
to me
11:53 AM
Google.support is not a legitimate address
Government-backed attackers may be trying to steal your password
There's a chance this is a false alarm, but we believe we detected government-backed attackers trying to steal your password. This happens to less than 0.1% of all Gmail users. We can't reveal what tipped us off because the attackers will take note and change their tactics, but if they are successful at some point they could access your data or take other actions using your account. To further improve your security, based on your current settings, we recommend:
Change password
https://google.com/amp/tinyurl.com/y7u8Wrle
The body of the email is real, but is being used to trick you.

Call IT FIRST.
Right away.
No Kidding.



Can the IT Department fix it, like it never really happened?
Not if you emailed information and not if the hacker got to the data first.
Then, there aren't going to be many remedies.

Alabama Data Breach Notification Act of 2018

(b) Notice to individuals under subsection (a) shall be made as expeditiously as possible and without unreasonable delay, taking into account the time necessary to allow the covered entity to conduct an investigation in accordance with Section 4. Except as provided in subsection (c), the covered entity shall provide notice within 45 days of the covered entity's receipt of notice from a third party agent that a breach has occurred or upon the covered entity's determination that a breach has occurred and is reasonably likely to cause substantial harm to the individuals to whom the information relates.

Alabama Data Breach Notification Act of 2018

Section 3.

(a) Each covered entity and third-party agent *shall implement and maintain reasonable security measures* to protect sensitive personally identifying information against a breach of security.

(b) Reasonable security measures means security measures practicable for the covered entity subject to subsection

(c) to implement and maintain, including consideration of all of the following:

1) ***Designation of an employee or employees to coordinate the covered entity's security measures*** to protect against a breach of security. An owner or manager may designate himself or herself.

2) ***Identification of internal and external risks of a breach of security.***

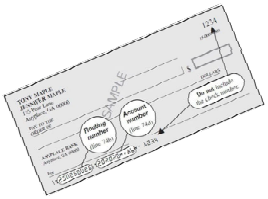
3) ***Adoption of appropriate information safeguards to address identified risks of a breach of security and assess the effectiveness of such safeguards.***

4) **Retention of service providers**, if any, that are **contractually required to maintain appropriate safeguards for sensitive personally identifying information.**

Change Procedures to Match the New Reality

- Tell your software company to remove the employee's ability to change their bank routing number or to implement 2-factor authentication for such changes.
- Make sure any change in routing number is followed by a paper paycheck for the next payroll*

*Risk still exists if the hacker can change the home address in the portal as well.



Make Rules for Direct Deposit Bank Account Changes

Real-World Authentication Rules

Since hackers can trick people into giving them information about themselves, don't trust emails and phone calls asking you to change account numbers.

Not for employees and not for businesses.

1. Email must come from their work account

   AND

2. Phone call must come from an extension within your school system

   AND

3. Someone that YOU know and that they know must verify they are asking for the change

High-Risk Access Requires Password Changes

Set rules that require those with NextGen access to change their passwords more frequently.

Anyone who can give such access to others should also change passwords more frequently.

HARRIS School Solutions

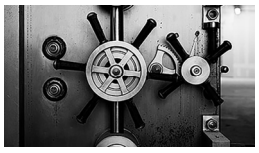
- Entering payment routing numbers for payments to vendors.
- Access to employee social security numbers.
- Access to changing direct deposit routing for employees.

Train New Employees!

Make sure they -

- Understand that they have a higher duty of care
- Undergo Phishing training
- Know your password policies
- Know your domain name
- Know your safety procedures for direct deposit and vendor ACH
- Know they are a target

Create a Culture of Shared Responsibility



Whose fault is it when employees fall for scams and give away their own login credentials?

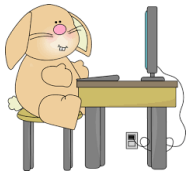
They need to be part of the shared responsibility.

Mixing work and personal life introduces more risk

"See? I told you it was possible to mix business with pleasure."

Checking Email at Home is Risky

- You are more likely to have saved personal login credential to your browser at home
- You may not have top-notch antivirus software on your home computer
- You won't be able to get in touch with the IT department during off hours



Don't Use Your Work Email for Personal Accts.

NETFLIX

amazon

facebook

ups

FedEx

If you stick to this, you will automatically know that an email is fake when it comes to your work email account.

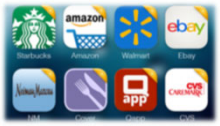
LinkedIn

Remove Saved Passwords from Web Browsers

Directions for removing saved passwords:

http://bit.ly/removepassword

Apps are the New Breeding Ground for Malware

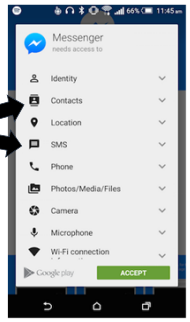


Hackers take advantage of popular apps, such as Pokémon Go. They create fakes and associated apps that offer help, storage, cheats, in order to infect the most phones.

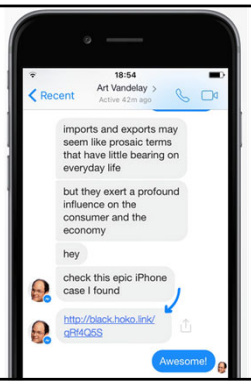
Try to get all apps from official app stores or official company websites -- not from individual websites or email links.

Read permissions before downloading – even for legitimate apps.

Read Reviews by former users and consider their ratings.



Once hackers get access to cell phone numbers they can send text messages that contain infected links or pictures to all your friends.



Infected Apps

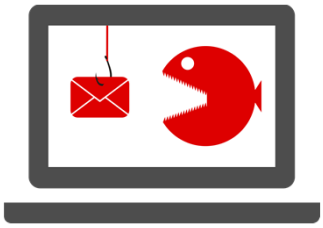
Warning Signs

- Weird text messages
- Unauthorized phone calls
- Unusually high data use
- Poor battery life and overheating
- Slow performance
- Redirects to Store
- Random popups

But are Special

Getting a lot of email is not a good enough reason to open up your System to cyber criminals.

Trying to be helpful is not a reason to open up your System to cyber criminals.



Falling for a phishing scam is

NOT OKAY.

ALABAMA LEADERS in EDUCATIONAL TECHNOLOGY

Susan.Poling@go-alet.org

References

- https://www.privacyrights.org/
- https://www.bbc.com/news/technology-44355153
- https://www.fbi.gov/contact-us/field-offices/portland/news/press-releases/fbi-tech-tuesdaybuilding-a-digital-defense-against-w-2-theft
- https://breachlevelindex.com/data-breach-mindset
- Google phishing quiz - https://phishingquiz.withgoogle.com/
- www. Splunk.com
- Source: https://www.myidcare.com/about-id-theft

Most images taken from Microsoft Creative Commons online library. Others used via Fair Use.

This presentation may not be made publicly available and may only be used for educational purposes.