Digital Learning Conference

July 25-26, 2018

Cybersecurity

Protecting You and Your Community from Cybercrime

James Costello, CISSP
Technology Security Specialist

Eric Pina
Technology Services

Jennifer Miller, CETL
Director of Technology Support Services/Performance Excellence

Today's Presentation

- CFISD Cybersecurity Team and Goals
- Cybercrime and Cybercriminals
- CFISD Cybersecurity Improvements
- Tips to Protect Students, Staff, and Community
- Questions, Comments, Concerns?

CFISD Cybersecurity Team

James Costello joined the Cy-Fair Technology team on February 19, 2018 as the Security Specialist.

James has over 20 years of experience working in Information Technology, in multiple industries. He is an active member of several IT Security organizations including InfraGard, ISC2, SecureWorld, etc.

James is a former student of Cy-Fair ISD and a resident of Cypress, and is extremely grateful for the opportunity to help improve the Cybersecurity Services for the district.

Certifications and Degrees: A+, Network +, Security+, and Certified Information Systems Security Professional certifications.

Associates in Networking Technology, a BBA from Texas State University, and is currently working towards a Master of Science in Information Assurance and Security from Sam Houston State University.

CFISD Cybersecurity Goals

To help students and staff to succeed in their tasks in a secure manner, and to protect our CFISD community from cybercrime.

Cybercrime and What's at Stake

What is Cybercrime?

Criminal activity or a crime that involves the Internet, a computer system, or computer technology.

What's at Stake for the CFISD Community?

- The ability for hardware and software to function as needed for students and staff to succeed.
- Sensitive information of students, staff, and their families.
- Legal action if Cy-Fair does not follow the federal and state regulations for protecting students, staff, and their data?

PII
Personally Identifiable Information

- PII is defined as information that can be used on its own or with other information to identify, contact, or locate an individual.

- The following data is often used to distinguish individual identity and is classified as PII: Name, Home Address, Email Address, Social Security #, Driver's License #, Date of Birth, Telephone Number, Login Name, Age, Gender, Race, Grades, etc.

Health Insurance Portability and Accountability Act - (HIPAA)

- HIPAA is a federal law that requires data privacy and security provisions for safeguarding medical information

- Penalties for HIPAA compliance violations can cost up to $1.5 million per incident!

FERPA
Family Educational Rights and Privacy Act

- Federal law regarding the safeguarding and confidentiality of information in a student's education record.

- Protects the access to and sharing of a student's education record, which is all information directly related to a particular student as part of his or her education.

- Guarantees that parents have access to their child's education record

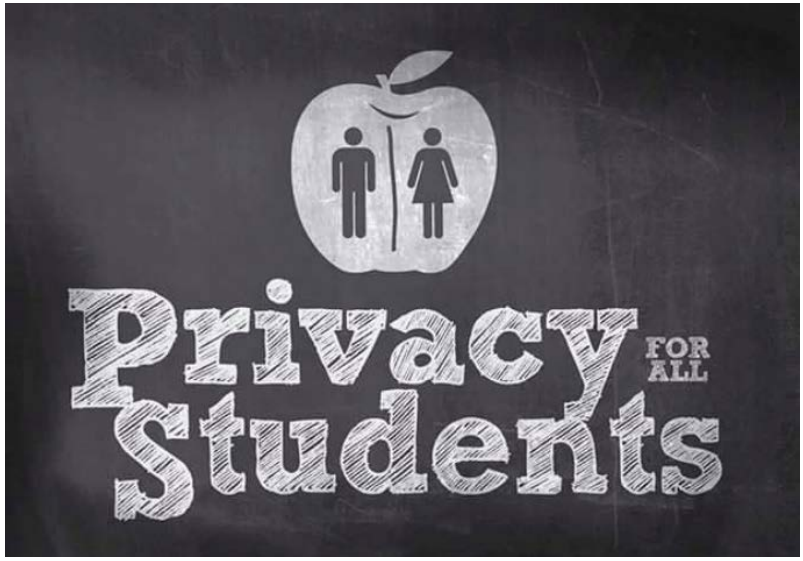
- Visit www.FerpaSherpa.org for some great information

COPPA
Children's Online Privacy Protection Act

- Controls the information collected from young children by companies operating websites, games, and mobile applications directed toward children **under 13**.
- Requires **companies** to have a **clear privacy policy**, **provide direct notice** to parents, and **obtain parental consent** before collecting information from children under 13.
- Teachers and other school officials authorized to provide consent on behalf of parents for use of an educational program, but **only for use in the educational context**.

PPRA
Protection of Pupil Rights Amendment

- Federal law which restricts what questions students might be asked for information as part of federally funded surveys or evaluations.



- Some specific areas include
  - Political affiliations
  - Mental and psychological problems potentially embarrassing to the student and his/her family
  - Religious practices, affiliations, or beliefs
  - Income (other than that required by law to determine eligibility for participation in a program or for receiving financial assistance under such program.)

CIPA
Children's Internet Protection Act

- Schools and libraries are required to adopt and implement an Internet safety policy addressing
  - Access by minors to inappropriate matter on the Internet;
  - The safety and security of minors when using electronic mail, chat rooms and other forms of direct electronic communications;
  - Unauthorized access, including so-called "hacking," and other unlawful activities by minors online;
  - Unauthorized disclosure, use, and dissemination of personal information regarding minors; and
  - Measures restricting minors' access to materials harmful to them.

Who are Cybercriminals?

- Computer geeks looking for bragging rights
- Hacktivists who are motivated by a political or social cause
- Businesses trying to gain an upper hand in the by hacking competitor websites
- Rings of criminals wanting to steal your personal information and sell it on black markets
- Spies and terrorists looking to rob our nation of vital information or launch cyber strikes.
- Criminals can include students

Examples of Cybercrime

- Phishing
- Ransomware
- Scareware
- Tech Support Scams
- Denial of Service Attacks

Phishing

- Fraudulent attempt to obtain sensitive information
  - Usernames
  - Passwords
  - Credit card details
  - Money
- For malicious reasons
- By disguising as a trustworthy entity in an electronic communication

Ransomware

- Insidious type of malware that encrypts, or locks, valuable digital files and demands a ransom to release them.
- No one is immune.
  - Hospitals
  - School districts
  - State and local governments
  - Law enforcement agencies
  - Small and large businesses

Ransomware

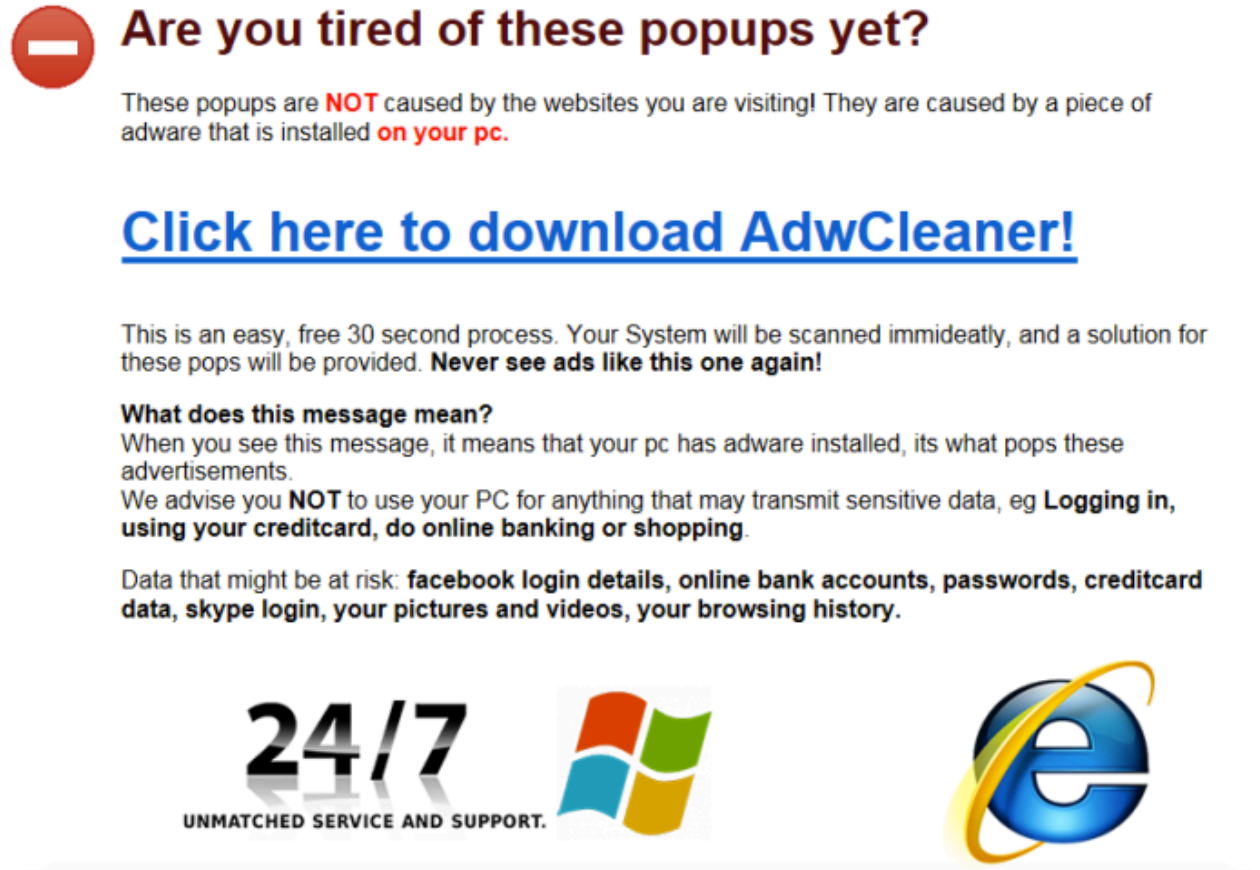
- How does it infect an organization?
  - Spreads via infected e-mail attachments or embedded URLs.
  - These phishing e-mails are designed to look like legitimate e-mail traffic.
  - The victim opens a malicious e-mail attachment or visits a compromised web site and the malware infects the victim's computer.
  - The ransomware can then spread across the network to any shared folder that employee has access to, encrypting all of the data in its path.

Scareware

- Malicious computer programs
- Designed to trick a user into buying and downloading unnecessary and potentially dangerous software
- Such as fake antivirus protection

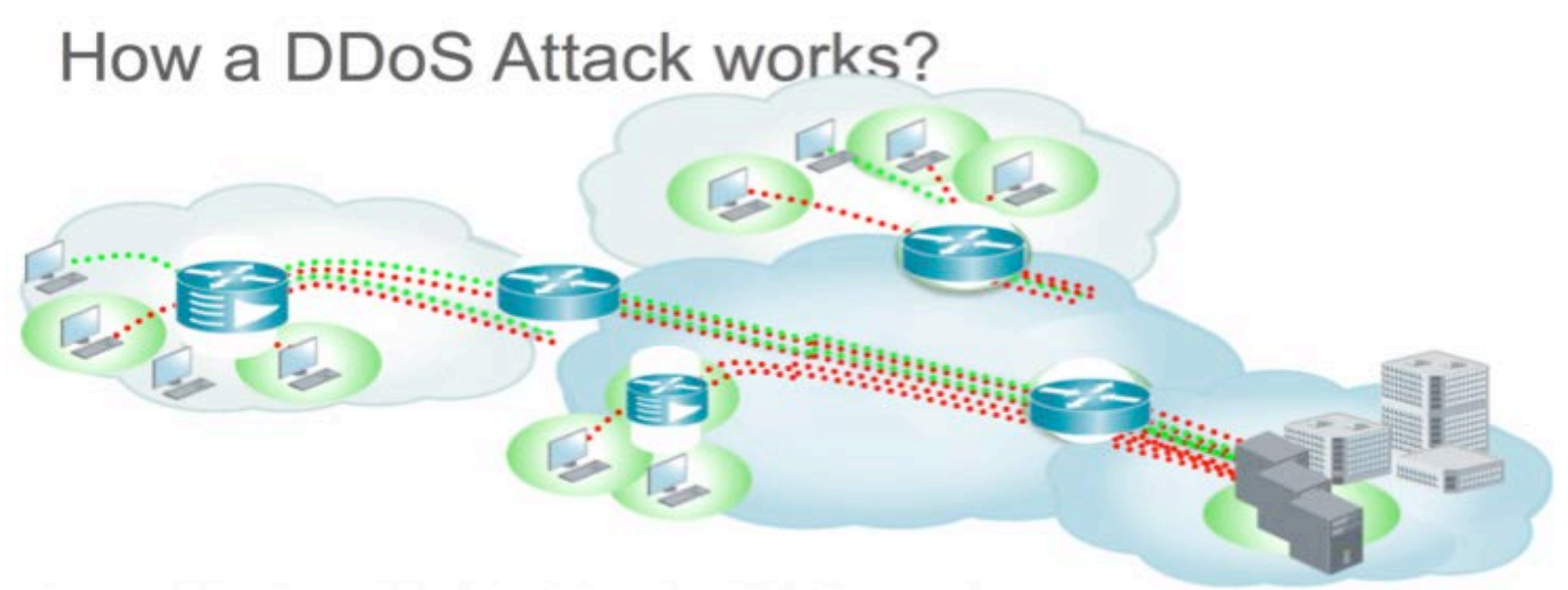
Tech Support Scams

- Scammers call and claim to be computer techs associated with well-known companies like Microsoft or Apple.
- Some send pop-up messages that warn about computer problems.
  - They've detected viruses or other malware on your computer
  - They claim to be "tech support"
  - Ask you to give them remote access to your computer
  - Diagnose a non-existent problem and ask you to pay for unnecessary – or even harmful – services



Dedicated Denial of Service Attacks

- Any type of attack where the attackers (hackers) attempt to prevent legitimate users from accessing the service.
- In a DoS attack, the attacker usually sends excessive messages asking the network or server to authenticate requests that have invalid return addresses.



K-12 Cybercrime in the News

Florida Virtual School Responds to Data Security Incident

A NOTICE TO STUDENTS AND PARENTS

Florida Virtual School (FLVS) recently learned of a potential data security incident involving certain information provided to us by students and parents. We are providing this notice as a precaution to inform potentially affected individuals about the incident and to call your attention to some steps you can take to help protect yourself. We sincerely regret any concern this may cause you.

FLVS learned that unauthorized individuals appear to have gained access to some of our computer systems that stored personal information relating to certain students, parents of students, and Leon County Schools' teachers. Although the investigation is still ongoing, based on what we have learned to date, we believe that this incident could affect information in FLVS school records, including but not limited to students' names, dates of birth, school account usernames and passwords, physical school identification, as well as parents' names and parent emails. We have not identified any evidence that any student or parent Social Security numbers or financial account information were affected. Please note, currently, we are not aware of any fraud or misuse of your information as a result of this incident.

The security incident may also affect a limited number of Leon County Schools' teachers, where the teachers' name, Social Security number, date of birth, address, phone number, cell phone number, emergency contact, spouse's name, personal email address, work email address, and certain demographic information, may have been accessed by unauthorized persons. These teachers are being directly notified by individual notice by Leon County Schools and FLVS is coordinating and cooperating with Leon County Schools in these efforts.

Click this link to view the News Channel 8 news story

K-12 Cybercrime in the News

TECHNOLOGY

High school student allegedly hacks school, charges fellow students to change grades

A 10th-grade student at Memorial High School in Houston is under arrest after allegedly hacking into his school's computer systems, changing grades and then charging other students to change to their own records.

The scheme, which started with a password stolen in an unspecified theft, ended on March 31 with an arrest by Spring Branch ISD police, according to local news reports.

"At this time, an ongoing investigation has found only one other underclassman paid the student to change their grades," a spokesperson said. The service, however, was allegedly advertised to others.

The student faces felony breach of computer security charges. In Texas, those charges automatically become felonies if the computers in question are government property, as the school's machines are.

K-12 Cybercrime in the News

- Tenafly High School – New Jersey - December 2017
  - High school student gained access to the IT systems
  - Changed the grades to improve his GPA
  - Sent out college applications immediately after
  - Also gained access to a nationwide IT system that allows colleges to access school records, grades, and other documents to evaluate applications.
  - Student had good grades but appears to have hacked the school due to the pressure of keeping his grades high and being accepted at an important college.

Tenafly High School.

K-12 Cybercrime in the News

News

Teen arrested for hacking into East Bay school district's computer system

Concord police shared this image Thursday, May 10, 2018 of a tissue box with an SD card inside that a K-9 specially trained in electronic-device location managed to recover in connection with an investigation.

CONCORD — An unnamed teenager was arrested this weekend in connection with an attack on a school district's computer system that resulted in grade changes for a number of students, authorities said Thursday.

Police responded to a call April 25 from Mt. Diablo Unified School District staff about an apparent intrusion, and later learned that a teacher clicked on a "phishing" e-mail, sending her credentials to a hacker.

That hacker then used the credentials to log into the district's computer system, changing grades for students. An investigation did not reveal any sign of stolen personally identifiable information.

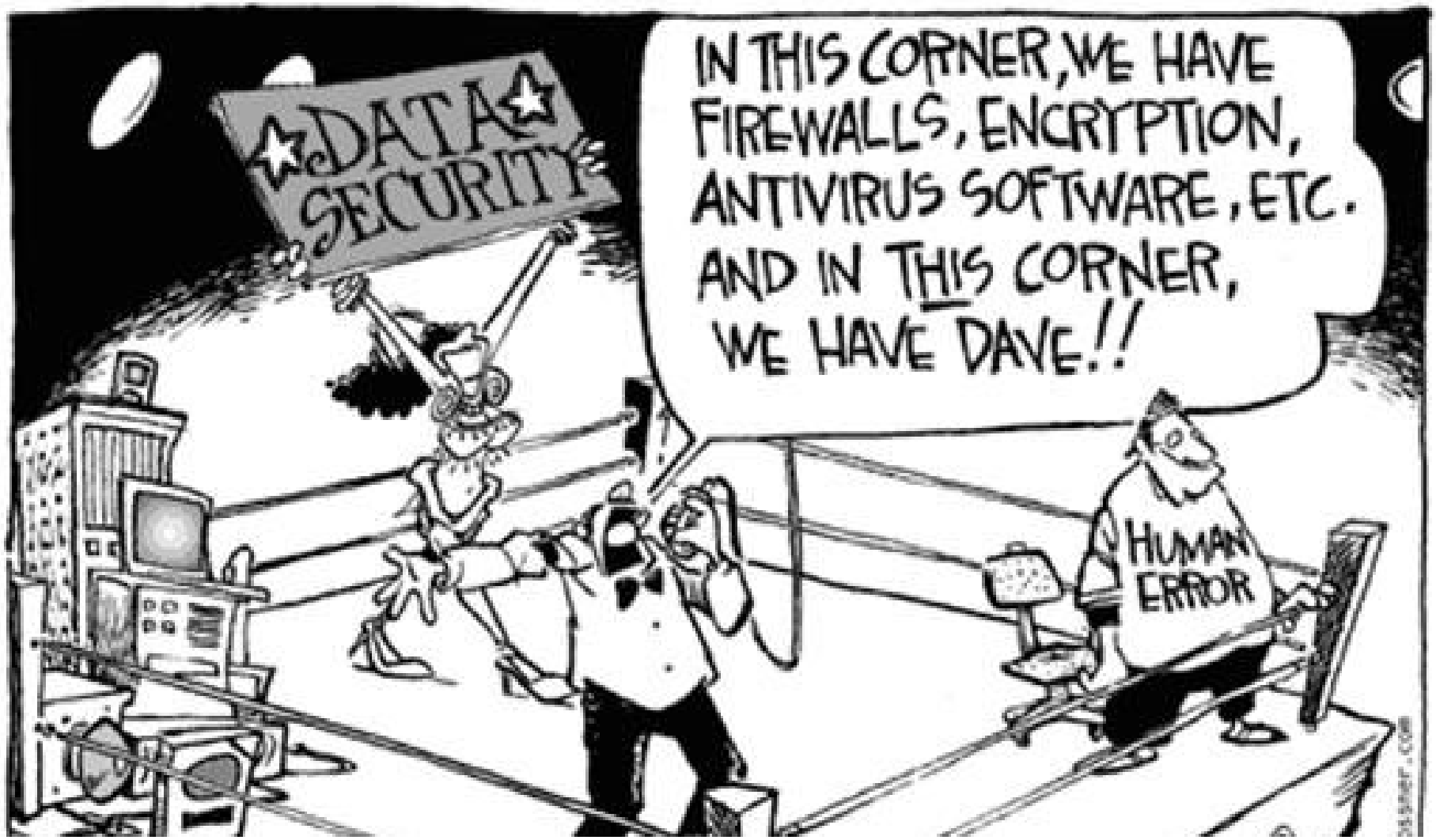
With help from the U.S. Secret Service, the Contra Costa County district attorney's office and Contra Costa County sheriff's officials, a teenager was arrested Wednesday after a search by a K-9 officer's "Dug," trained in electronic-device detection, yielded an SD card hidden in a tissue box.

According to KGO-TV, Ygnacio Valley High School sophomore David Rotaro, 16, admitted to the hack, saying he had sent the e-mail to staff and used the retrieved username and password to raise or drop grades of 10 to 15 people, but not his own grades. Rotaro, who was released from custody Wednesday, told the TV station "it was like stealing candy from a baby."

Cybersecurity Improvements at CFISD

- Planned Implementations
  - Microsoft Advanced Threat Protection
  - Multifactor Authentication options
  - Content Filters
  - SpyCloud
  - External Email Warning Banner
- Software support
  - Enterprise Level Anti-malware
  - Hard drive encryption
- Vendor support
- Software Review
- Data Privacy Agreement
- DHS Engagement
- Training
  - Phish Alert Button
  - KnowBe4 Training
- Improved Security Related Communications
- Updated website
- Continuous Policy Review

Protection from Cybercrime



Questions to help you evaluate whether an app, website, product, or service will protect your student's information

1. Does the product collect Personally Identifiable Information? ·
   - FERPA, the federal privacy law applies to "**education records**" only, but many state laws cover ALL student personal information.
2. Does the vendor commit not to further share student information other than as needed to provide the educational product or service?
   - The vendor should **clearly promise never to sell data**.
3. Does the vendor create a profile of students, other than for the educational purposes specified?
   - Vendors are **not allowed to create a student profile for any reason outside of the authorized educational purpose**.
4. When you cancel the account or delete the app, will the vendor delete all the student data that has been provided or created?

Questions to help you evaluate whether an app, website, product, or service will protect your student's information

5. Does the product show advertisements to student users?
   - Ads are allowed, but many states ban ads targeted based on data about students or behavioral ads that are based on tracking a student across the web. These are **never acceptable** for school use.
6. Does the vendor allow parents to access data it holds about students or enable schools to access data so the school can provide the data to parents in compliance with FERPA?
7. Does the vendor promise that it provides appropriate security for the data it collects?
   - A particularly secure product **will specify that it uses encryption when it stores or transmits student information**. Encrypting the data adds a critical layer of protection for student information and indicates a higher level of security.

Questions to help you evaluate whether an app, website, product, or service will protect your student's information

8. Does the vendor claim that it can change its privacy policy without notice at any time?
   - This is a red flag— current **FTC rules require that companies provide notice to users when their privacy policies change in a significant or "material" way, and get new consent for collection and use of their data**.
9. Does the vendor say that if the company is sold, all bets are off?
   - The policy should state that **any sale or merger will require the new company to adhere to the same protections**.
10. Do reviews or articles about the product or vendor raise any red flags that cause you concern?

Submit a service request through iSupport to ensure the website or application is appropriate for classroom use if it requests student information.

TXSPA Database

Cypress-Fairbanks ISD

City: Houston | Contact: James Costello | Phone: 281-897-4357 | Email: DPA@cfisd.net

Status Key	**Active:** Contract is signed and app is in use. **Declined:** Vendor was unable to sign the contract and the app is not in use.

GUEST

More Info

Learn about TXSPA
View Participating Districts
Member Login

Texas Student Privacy Alliance

Show 10 entries Search:

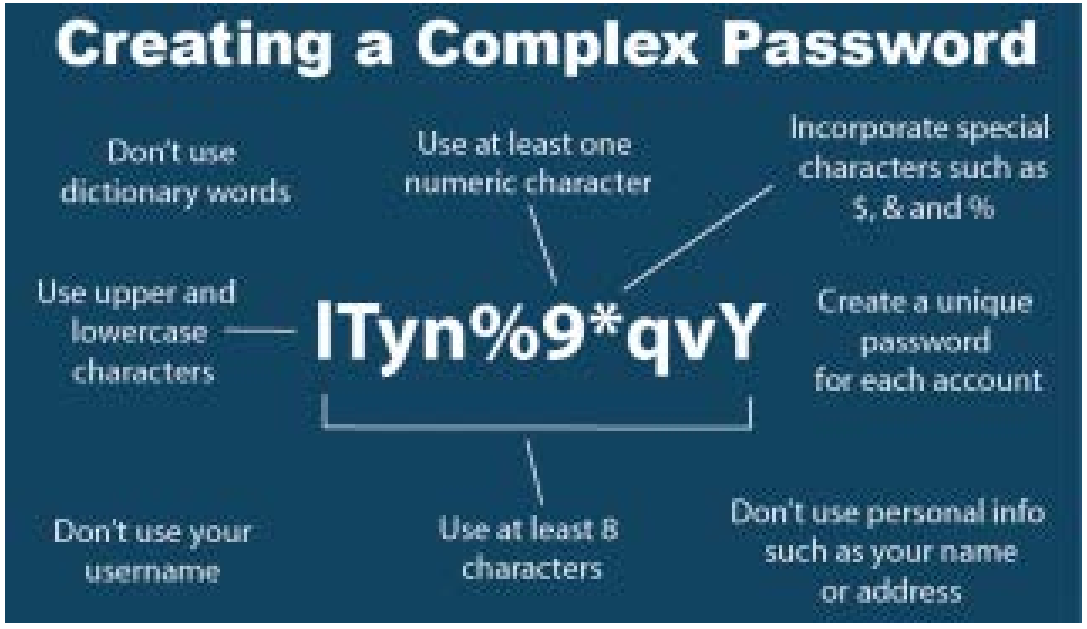
Software Name	Agreement Status	Agreement Type	Agreement Dates	Grade Level	Content Area	Data
Achieve 3000	Active	District Modified	Approved: 2018-06-11			
Aesop	Approved (No Data Collected)	Vendor-Specific	Approved: 2018-03-28			
Amplify	Active	District Modified	Approved: 2018-05-21			
Animoto	Not Approved	Declined				

- Active Contracts
- Approved (No Data Collected)
- Not Approved

Approved Software Database

Protection and Prevention

- Adhere to Policies and Procedures
  - Software installation requests
  - Application approval
  - Responsible Use Agreement
  - Complex Password Adherence



Additional Information

Type: Equipment; Software or App - Purchased or Free; Both

Item to Purchase: --Select--

Cost:

Paid by:

Principal:

Grade Level - Press CTRL to select multiple: EE, PK, K, 1

Content Area - Press CTRL to select multiple: English Language Arts, Health, Instructional Technology, Library Media

How do you envision students using the resource?:

Protection and Prevention

- Contact the Customer Care Center with suspicious incidents
  - Forward suspicious emails as attachments to iSupport@cfisd.net
  - Report unusual login prompts
  - Call 281-897-4357
  - Email isupport@cfisd.net

For immediate assistance, please contact our Customer Care Center at 281-897-4357

- Do not leave your logged in computer unattended

Lock

Protection and Prevention

- Secure files containing student information
- Use your work email only for work
  - This helps to reduce the damage of a compromised account.
- Information security
  - If you don't need it, don't keep it.
  - If you do need it, keep it someplace secure, and not in your email.
- Utilization of network drives and cloud space
  - S:, H:
  - Google drive, One Drive
- Don't carry student data on unencrypted USB drives

Protection and Prevention

Social Engineering Red Flags

FROM

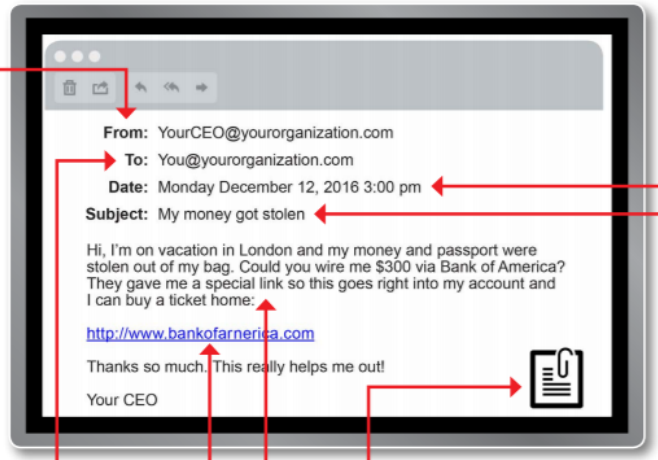
- I don't recognize the sender's email address as someone **I ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address from a **suspicious domain** (like micorsoft-support.com)?
- **I don't know the sender personally** and they **were not vouched for** by someone I trust.
- **I don't have a business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I haven't communicated with recently.

TO

- I was cc'd on an email sent to one or more people, but **I don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a **big** red flag.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, www.bankofarnerica.com — the "m" is really two characters — "r" and "n."



DATE

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?

SUBJECT

- Did I get an email with a subject line that is **irrelevant** or **does not match** the message content?
- Is the email message a reply to something **I never sent or requested**?

ATTACHMENTS

- The sender included an email attachment that **I was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**. The only file type that is **always safe to click on is a .txt** file.

CONTENT

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar** or **spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd** or **illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?

Protection and Prevention

- Use complex passwords
  - Provide more protection for academic email accounts
  - Change your personal passwords regularly
  - Use unique passwords
  - Mix uppercase, lowercase, numbers and special characters
  - Make the password as long as the system allows
  - Use passphrases instead of passwords
  - Never share passwords with others

Nonrandom/Unsecure

- Cat in the hat
- My beautiful red house

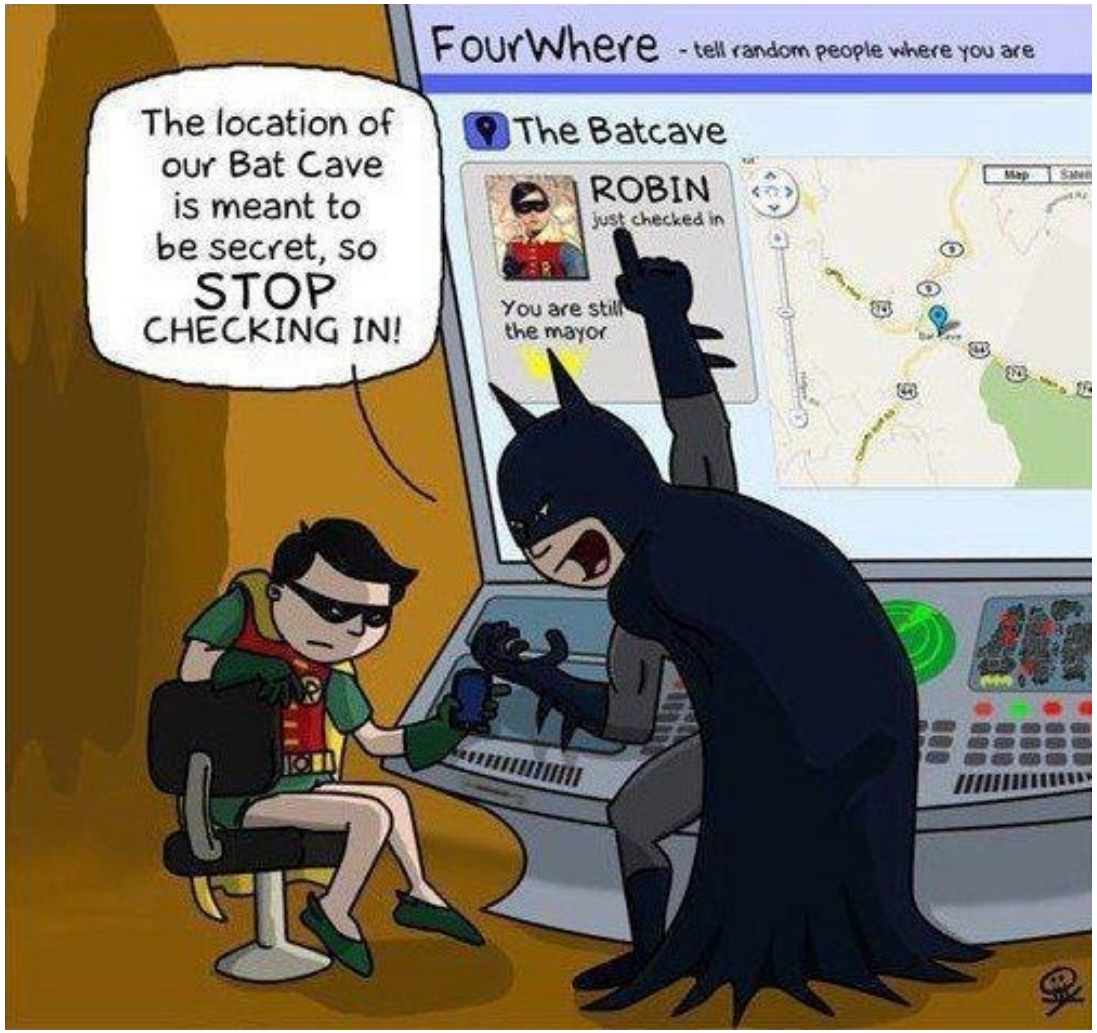
Common phrases
Word order makes sense
Makes grammatical sense

Random/Secure

- C0rrecth0rsebattery
- Seash3llglar1ng

Doesn't make sense
Is not grammatically correct
Uses numbers in place of letters

How to Protect your Families and Community



How to Protect your Families and Community

- Social Media
  - Posting of business or vacation travel notifies scammers when people are out of reach
  - Provides information about friends, family, and business deals
  - Be wary of innocent appearing games/questionnaires – provide common answers to security questions
  - Verify privacy settings
- Email
  - If you suspect suspicious activity, change your password immediately
  - Check for any new rules in your account

How to Protect your Families and Community

- Be Cautious with your Downloads
  - Carelessly downloading e-mail attachments can circumvent even the most vigilant anti-virus software.
  - **Never** open an e-mail attachment from someone you don't know
  - ***Be wary*** of forwarded or unexpected attachments from people you do know. They may have unwittingly advanced malicious code included.

How to Protect your Families and Community

- Viruses can infect computers without users' knowledge.
- Utilize Antivirus Software
  - Designed to prevent malicious software programs from embedding on your computer.
  - If it detects malicious code, it works to disarm/remove it.
  - Update as recommended
- Backups
  - Save your files in multiple locations
  - Review regularly
  - Ensure backups are not connected to the computers and networks they are backing up as these are becoming targets of ransomware.

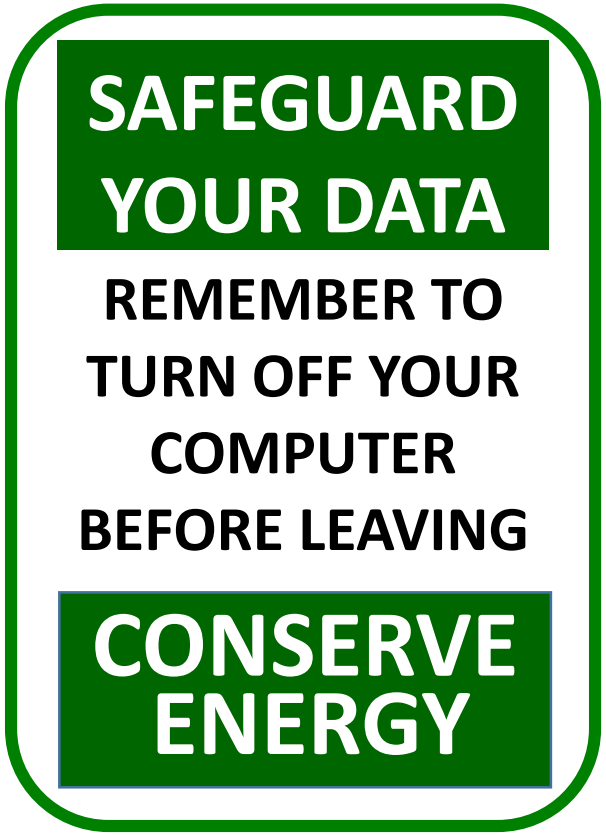
How to Protect your Families and Community

- Patching/Updates
  - Keep Your Operating System Up to Date
  - Computer operating systems are periodically updated to stay in tune with technology requirements and to fix security holes.
  - Install the updates to ensure your computer has the latest protection.

- Report any suspicious activity to local law enforcement

How to Protect your Families and Community

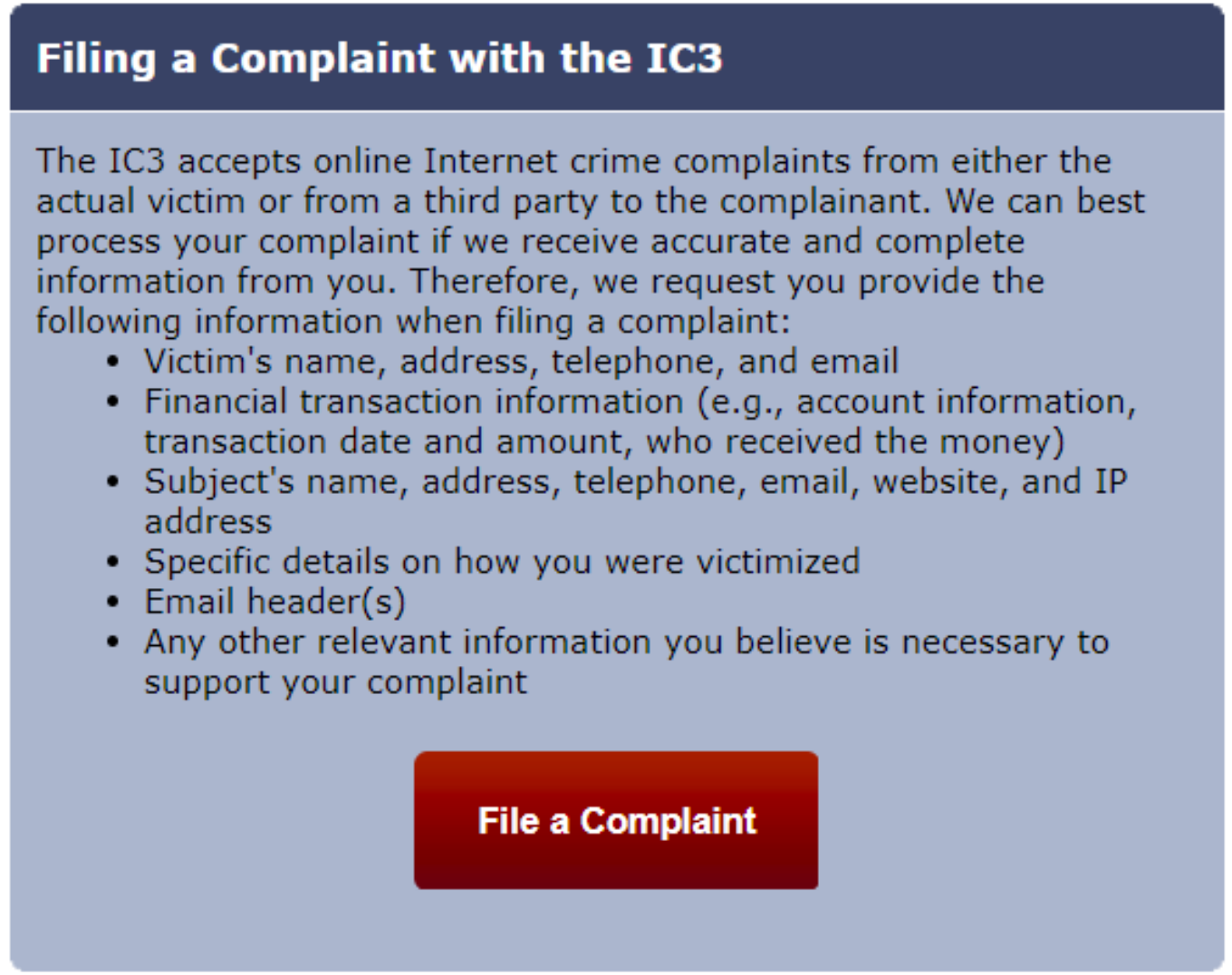
- Turn Off Your Computer
  - Being “always on” renders computers more susceptible
  - Powering off the computer, effectively severs an attacker’s connection
- Change the default username and password for your devices
- Keep Your Firewall Turned On
  - A firewall helps protect your computer from hackers who might try to gain access to crash it, delete information, or even steal passwords or other sensitive information.



How to Protect your Families and Community

- Utilize the Internet Crime Complaint Center (IC3) if you become the victim of cybercrime

- www.ic3.gov



How to Protect your Families and Community

Protecting Your Children Online

- Keep Communication Lines Open
- “Friend” your children on social media
- Limit “alone” time with devices – cell phones, computers, tablets
  - Use charging station in central location at night
- Pattern appropriate behavior
- Utilize applications to monitor phone use

Freeze Your Child’s Credit

Contact the three credit reporting agencies directly.

Equifax, TransUnion and Experian

- Ask them to create a credit report.
- Immediately put a freeze on it.
- Fee may be charged

Questions?

What do you think?

You receive an email from your bank informing you that it suspects an unauthorized transaction on your account. To protect your account, the email advises you to click on a link to verify your identity. Should you do so?

No way – the whole thing sounds 'phishy'! If you're concerned about your account, contact your bank directly using a phone number or Web address you know is genuine.

Yes. If someone is using your bank account, you don't have a second to lose. Immediately click on the link to verify your identity.

Yes – but first you should make sure the message looks like it's legitimate.

https://www.consumer.ftc.gov/sites/www.consumer.ftc.gov/files/games/off-site/ogol/_phishing-scams.html

Correct

You receive an email from your bank informing you that it suspects an unauthorized transaction on your account. To protect your account, the email advises you to click on a link to verify your identity. Should you do so?

No way – the whole thing sounds 'phishy'! If you're concerned about your account, contact your bank directly using a phone number or Web address you know is genuine.

Exactly. Not only should you refuse to click on the link, which could expose you to viruses and spyware, but, if you think someone is 'phishing' for your personal information, forward the email to spam@uce.gov and also to the company, bank or organization that was being impersonated.

https://www.consumer.ftc.gov/sites/www.consumer.ftc.gov/files/games/off-site/ogol/_phishing-scams.html

Incorrect

You receive an email from your bank informing you that it suspects an unauthorized transaction on your account. To protect your account, the email advises you to click on a link to verify your identity. Should you do so?

Yes. If someone is using your bank account, you don't have a second to lose. Immediately click on the link to verify your identity.

Sorry, that's just what 'phishin' scam artists want you to do….but it's dangerous – clicking on links in some emails can expose you to viruses and spyware. If you're concerned about your account, contact your bank using a phone number you know is genuine, or open a new Internet browser session and type in the company's correct Web address yourself.

https://www.consumer.ftc.gov/sites/www.consumer.ftc.gov/files/games/off-site/ogol/_phishing-scams.html

Incorrect

You receive an email from your bank informing you that it suspects an unauthorized transaction on your account. To protect your account, the email advises you to click on a link to verify your identity. Should you do so?

Yes – but first you should make sure the message looks like it's legitimate.

That could be risky. 'Phishing' scam artists are very good at looking and sounding official, but if you click on a link in some emails, you could be unleashing viruses or spyware on your computer. If you're concerned about your account, contact your bank using a phone number you know is genuine, or open a new Internet browser session and type in the company's correct Web address yourself.

https://www.consumer.ftc.gov/sites/www.consumer.ftc.gov/files/games/off-site/ogol/_phishing-scams.html

What do you think?

You're surfing the Web when you see a pop-up message from your Internet Service Provider (ISP) saying that it needs you to click on a link to verify or update your account information. Should you comply?

It sounds like a reasonable request, so click on the link to see what type of information they need from you, and follow the instructions.

Just say no. Legitimate companies, including ISPs, never ask for this information via pop-up ads or email.

Reply immediately. If you don't cooperate, you could run the risk of losing all your email messages, and possibly even being permanently disconnected from the Internet.

https://www.consumer.ftc.gov/sites/www.consumer.ftc.gov/files/games/off-site/ogol/_phishing-scams.html

Correct

You're surfing the Web when you see a pop-up message from your Internet Service Provider (ISP) saying that it needs you to click on a link to verify or update your account information. Should you comply?

Just say no. Legitimate companies, including ISPs, never ask for this information via pop-up ads or email.

You're right on the money: you should never respond to such messages. Instead, close the pop-up by clicking on the "X" in the corner of the ad window.

https://www.consumer.ftc.gov/sites/www.consumer.ftc.gov/files/games/off-site/ogol/_phishing-scams.html

Incorrect

You're surfing the Web when you see a pop-up message from your Internet Service Provider (ISP) saying that it needs you to click on a link to verify or update your account information. Should you comply?

It sounds like a reasonable request, so click on the link to see what type of information they need from you, and follow the instructions.

Sorry, you need to be more cautious. Legitimate companies never ask for account or other personal information via pop-up ads or email, so you should never reply to such messages, nor click on links they may contain. Close the pop-up window by clicking the "X" in the corner of the ad window.

https://www.consumer.ftc.gov/sites/www.consumer.ftc.gov/files/games/off-site/ogol/_phishing-scams.html

Incorrect

You're surfing the Web when you see a pop-up message from your Internet Service Provider (ISP) saying that it needs you to click on a link to verify or update your account information. Should you comply?

Reply immediately. If you don't cooperate, you could run the risk of losing all your email messages, and possibly even being permanently disconnected from the Internet.

Sorry, you need to be more cautious. Legitimate companies never ask for account or other personal information via pop-up ads or email, so you should never reply to such messages, nor click on links they may contain. Close the pop-up window by clicking the "X" in the corner of the ad window.

https://www.consumer.ftc.gov/sites/www.consumer.ftc.gov/files/games/off-site/ogol/_phishing-scams.html

What do you think?

Despite all your precautions, let's say you suspect that you've been 'phished' – and provided personal or financial information to someone masquerading as your ISP, bank, online payment service, or even a government agency. What should you do?

Not to worry. Because you gave your information in good faith, there's no way doing so could cause any harm.

Contact your local marine sports licensing board to see whether the company has a valid phishing license.

First, file a complaint at ftc.gov. Then, since phishing victims can also become victims of identify theft, visit the FTC's Identify Theft website for more information at www.consumer.gov/idtheft.

https://www.consumer.ftc.gov/sites/www.consumer.ftc.gov/files/games/off-site/ogol/_phishing-scams.html

Correct

Despite all your precautions, let's say you suspect that you've been 'phished' – and provided personal or financial information to someone masquerading as your ISP, bank, online payment service, or even a government agency. What should you do?

First, file a complaint at ftc.gov. Then, since phishing victims can also become victims of identify theft, visit the FTC's Identify Theft website for more information at www.consumer.gov/idtheft.

Nice catch! Another smart step is to review a free copy of your credit report periodically to look for any new account activity. See www.annualcreditreport.com.

https://www.consumer.ftc.gov/sites/www.consumer.ftc.gov/files/games/off-site/ogol/_phishing-scams.html

Incorrect

Despite all your precautions, let's say you suspect that you've been 'phished' – and provided personal or financial information to someone masquerading as your ISP, bank, online payment service, or even a government agency. What should you do?

Contact your local marine sports licensing board to see whether the company has a valid phishing license.

Unfortunately, that's incorrect. If you think you've been phished, file a complaint at ftc.gov, then visit the FTC's Identify Theft website, at www.consumer.gov/idtheft. It could also help to review a free copy of your credit report periodically to look for any new account activity.

https://www.consumer.ftc.gov/sites/www.consumer.ftc.gov/files/games/off-site/ogol/_phishing-scams.html

Incorrect

Despite all your precautions, let's say you suspect that you've been 'phished' – and provided personal or financial information to someone masquerading as your ISP, bank, online payment service, or even a government agency. What should you do?

Not to worry. Because you gave your information in good faith, there's no way doing so could cause any harm.

Unfortunately, that's incorrect. If you think you've been phished, file a complaint at ftc.gov, then visit the FTC's Identify Theft website, at www.consumer.gov/idtheft. It could also help to review a free copy of your credit report periodically to look for any new account activity.

https://www.consumer.ftc.gov/sites/www.consumer.ftc.gov/files/games/off-site/ogol/_phishing-scams.html

What do you think?

Let's say you work for an organization with an excellent information technology office. Your network administrator sends you an email warning of a security breach and asking you to confirm your password by entering it into a secure website. What should you do?

Don't share your password or any other personal information. Report the incident by calling your IT office or by emailing them at an address you know to be genuine

Don't enter your password on the website. Instead, send your reply by email to the sender.

Immediately enter your password on the website. You can always trust emails from your organization.

https://www.consumer.ftc.gov/sites/www.consumer.ftc.gov/files/games/off-site/ogol/_phishing-scams.html

Correct

Let’s say you work for an organization with an excellent information technology office. Your network administrator sends you an email warning of a security breach and asking you to confirm your password by entering it into a secure website. What should you do?

Don’t share your password or any other personal information. Report the incident by calling your IT office or by emailing them at an address you know to be genuine

Congratulations! You’ve successfully avoided a ‘spear phishing’ attack, where an attacker sends phishing messages that appear to be from a powerful or trusted person or office within an organization. You should be wary of any email that asks you to share personal or financial information.

https://www.consumer.ftc.gov/sites/www.consumer.ftc.gov/files/games/off-site/ogol/_phishing-scams.html

Incorrect

Let’s say you work for an organization with an excellent information technology office. Your network administrator sends you an email warning of a security breach and asking you to confirm your password by entering it into a secure website. What should you do?

Don’t enter your password on the website. Instead, send your reply by email to the sender.

You’ve been targeted by a ‘spear phishing’ attack, where an attacker sends phishing messages that appear to be from a powerful or trusted person or office within an organization. Report the incident by calling your IT office or emailing them at an address you know to be genuine. In any case, email is not a secure tool for sharing passwords or other personal information.

https://www.consumer.ftc.gov/sites/www.consumer.ftc.gov/files/games/off-site/ogol/_phishing-scams.html

Incorrect

Let’s say you work for an organization with an excellent information technology office. Your network administrator sends you an email warning of a security breach and asking you to confirm your password by entering it into a secure website. What should you do?

Immediately enter your password on the website. You can always trust emails from your organization.

You’ve been targeted by a ‘spear phishing’ attack, where an attacker sends phishing messages that appear to be from a powerful or trusted person or office within an organization. Report the incident by calling your IT office or emailing them at an address you know to be genuine. In any case, email is not a secure tool for sharing passwords or other personal information.

https://www.consumer.ftc.gov/sites/www.consumer.ftc.gov/files/games/off-site/ogol/_phishing-scams.html

What do you think?

OnGuard Online suggests several ways to avoid getting hooked by a phishing scam, including reviewing credit card and bank account statements as soon as you receive them. How can this help you avoid being scammed?

It's a quick way to make sure you're solvent. If you have money in the bank, or credit, you're still a player!

By reviewing your statements for unauthorized charges, you can know quickly whether someone has started using your account. If this happens, you can alert authorities and stop the problem before more damage occurs.

It's not that it helps directly, but it will give you something to do while waiting to see if the scammers have drained your account.

https://www.consumer.ftc.gov/sites/www.consumer.ftc.gov/files/games/off-site/ogol/_phishing-scams.html

Correct

OnGuard Online suggests several ways to avoid getting hooked by a phishing scam, including reviewing credit card and bank account statements as soon as you receive them. How can this help you avoid being scammed?

By reviewing your statements for unauthorized charges, you can know quickly whether someone has started using your account. If this happens, you can alert authorities and stop the problem before more damage occurs.

You are correct. Here's another tip: if your statement is late by more than a couple of days, call your credit card company or bank to confirm your billing address and account balances. Better safe than sorry!

https://www.consumer.ftc.gov/sites/www.consumer.ftc.gov/files/games/off-site/ogol/_phishing-scams.html

Incorrect

OnGuard Online suggests several ways to avoid getting hooked by a phishing scam, including reviewing credit card and bank account statements as soon as you receive them. How can this help you avoid being scammed?

It's a quick way to make sure you're solvent. If you have money in the bank, or credit, you're still a player!

This technique helps by allowing you to spot potentially fraudulent use of your account while there may still be time to control the damage. If your statement is late by more than a couple of days, call your credit card company or bank to confirm your address and account balances.

https://www.consumer.ftc.gov/sites/www.consumer.ftc.gov/files/games/off-site/ogol/_phishing-scams.html

Incorrect

OnGuard Online suggests several ways to avoid getting hooked by a phishing scam, including reviewing credit card and bank account statements as soon as you receive them. How can this help you avoid being scammed?

It's not that it helps directly, but it will give you something to do while waiting to see if the scammers have drained your account.

This technique helps by allowing you to spot potentially fraudulent use of your account while there may still be time to control the damage. If your statement is late by more than a couple of days, call your credit card company or bank to confirm your address and account balances.

https://www.consumer.ftc.gov/sites/www.consumer.ftc.gov/files/games/off-site/ogol/_phishing-scams.html

Questions?