CYBERSECURITY TIPS AND TOOLS- A GUIDE ON CYBER ATTACKS AND MALWARE

Frosty Walker

Chief Information Security Officer

Texas Education Agency

Frosty.Walker@tea.texas.gov

(512) 463-5095

Data Security Advisory Committee

The Data Security Advisory Committee (DSAC) provides guidance to the Texas education communities, maximizing collaboration and communication regarding information security issues and resources which can be utilized within the educational communities served.

The DSAC is currently comprised of representatives from school districts, ESCs, TEA and the private sector.

Texas Gateway

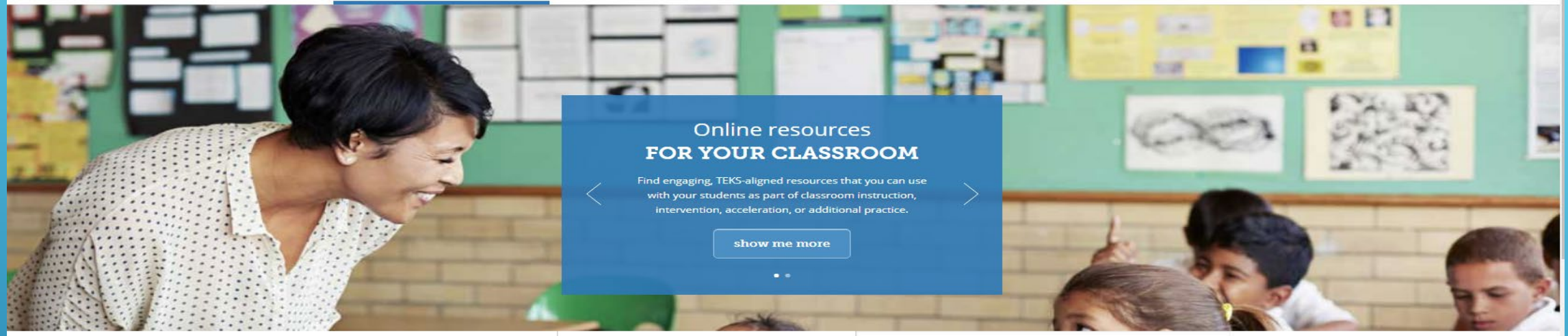
https://www.texasgateway.org/

Cybersecurity Tips and Tools

Secure | https://www.texasgateway.org

TEA | TEA WEBSITE | CONTACT TEA | SIGN UP FOR UPDATES

Texas Gateway for online resources by TEA | TEKS | SEARCH | MORE | Log in | Sign Up



BROWSE TEKS | BROWSE RESOURCES | Search

Featured Resources

1 of 2

EARLY CHILDHOOD

Prekindergarten Enrollment Toolkit

ESTAR/MSTAR

MATH

ESTAR/MSTAR

2

Open-Source Instructional Materials

openstax STUDY EDGE TEA

cybersecurity data

Cybersecurity Tips and Tools

Restorative Discipline Practices in Texas

4

ELA & READING

Complete "Red Book Series" Focused on Reading Instruction

TEXAS LESSON STUDY

Texas Lesson Study Briefing

Starting the Conversation

16

MATH

TEA Statistics

Statistics

TEA

Cyber Attacks and Malware

Malware, short for malicious software, refers to any malicious coding that can infiltrate a computer. There are many types of malware, with the list of types growing rapidly as new and manipulated versions of existing forms are discovered.

Viruses

Pure computer viruses constitute pieces of malicious code or an entire program attaching itself to files. This causes the affected file to duplicate itself, in much the same way as a physical virus duplicates itself inside a living cell.

A virus is activated once the file or program that it inhabits is opened or begins running. This can go on to affect other computers on the same network to potentially devastating effects.

There is a variety of anti-virus software available, some being available for free, although they can be basic compared to purchased programs. Anti-virus software should be utilized on PC's, laptops, tablets, and mobile phones.

Security Awareness programs

Trojans

One of many varieties of viruses, trojans, or Trojan Horses, are pieces of malware that masquerade as a harmless program. Its name is derived from the Trojan Horse described by Homer during his account of the fall of Troy.

Once activated, trojans are capable of copying, manipulating, blocking and deleting data, as well as slowing down the device they occupy. Trojans can take plenty of forms, including:

- Backdoor: This involves the creation of a ‘backdoor’ that cyber attackers can use to upload and delete data and download more malware. Attackers using backdoor trojans can also work together to manipulate an entire network.
- Downloader: Downloader trojans can download and install new versions of malicious programs that are infested with malware.
- Infostealer: This type of trojan can be implemented in order to steal personal information from a computer.
- Remote Access: Like a backdoor but with more capabilities, this gives attackers full control over the computer.

Worms

Worms are a type of malware virus that can replicate without any user intervention. These copies can then spread throughout the user's network, including emails and instant messages, without the user knowing.

This type of malware exploits vulnerabilities within network protocols. Additionally, worms can be transported via a USB drive or CD.

In addition to the pure computer worm, hybrids of worms and viruses that can modify program code like a virus, are common.

Worms can also operate as part of a botnet with other worms in order to take complete control of a network.

Ransomware

Ransomware is a type of malware that involves access to a computer's data being encrypted, and the attacker demanding money, usually in the form of cryptocurrency in order to conceal the culprit's identity, to unlock the data again.

Initially, ransomware attackers used software for sale on the dark web to implement this kind of malware, but this is now possible with little to no technical background and at a lower cost thanks to the increasing availability of ransomware-as-a-service (RaaS).

Ransomware can be spread via emails, infiltrated applications and websites, or even through remote desktop protocols.

The approaches that ransomware attackers utilize include:

-pop-up messages threatening to destroy encryption keys to data unless victims pay them money,

-scam emails regarding 'illegal' software on the victim's computer along with an electronic fine,

-the sale of software that the attacker promises will unlock encryption that's locking a victim's data, which the attacker placed on it in the first place.

Malvertising

Malvertising is malware that can be found within online advertisements. They can be found on most popular websites that have third-party advertising.

Cyber attackers using this method will either implement pop-up ads straight onto a site, commonly with messages referring to awards that the user has ‘won’ and similar varieties, or insert malware into legitimate advertisements after a few months of those advertisements being on the website.

Drive-by Downloads

Drive-by downloads are small pieces of malware that are hidden by attackers within websites that will probably seem completely innocent. Usually, there are many kinds of malware present on one site, implemented in the hope of exploiting a weakness in the user's computer.

Culprits of this type of cyber attack usually make use of an exploit kit that can find websites that are vulnerable.

As soon as these sites are visited, these pieces of malware are secretly downloaded onto the user's device, hence the 'drive-by' aspect of the attack's name.

These pieces of malware contact another computer in order to introduce the rest of the coding they need to access the rest of the computer or mobile device.

Phishing

Phishing typically involves attackers obtaining a victim's personal information. This can include log-in and bank details. Phishing attempts can be made via email, over the phone (**Vishing**: short for 'voice phishing'), or in the form of a text message (**Smishing**: short for 'sms phishing').

Phishing attackers masquerade as another person or entity that the victim may think has a legitimate and innocent need for their personal details.

These attacks put an emphasis on victims giving key information to attackers.

Phishing attacks often involve a combination of authentic-looking emails from a highly ranked and respected official and suggest a sense of urgency concerning the need for information or funding.

The person who the attacker impersonates is often a senior colleague.

Spear Phishing

Spear phishing involves sending personalized messages to particular victims, making these messages seem more legitimate and innocent in the eyes of the receiver. This makes the technique more likely to successfully steal personal information.

In addition to asking for personal details, messages may also be infested with links laced with malware, which can be downloaded onto a victim's device if the link is clicked on.

Attackers can research the victim's hometown, place of work, network of employees or friends, in the process, constructing a supposedly believable email.

Messages addressed to entire organizations are also common.

Business Email Compromise (BEC)

A business email compromise, or BEC, is any method of email phishing that involves attackers pretending to be business executives or business associates in an aim to gain access to classified data from employees, customers or vendors.

In one type of BEC, attackers masquerade as a company executive in order to obtain funds or sensitive information. These BEC attempts are made to look convincing, at first by gaining access to an executive's email account, then addressing a particular target after searching the executive's emails and social media accounts.

The emails typically feature a sense of urgency, ordering the target to transfer money or data over immediately.

Types of Business Email Compromise (BEC)

- A bogus invoice scam, which involves cyber criminals disguised as company executives ordering the company's finance department to change the destination of a payment to that of the attacker ahead of a due invoice.
- An account compromise, in which attackers hack an employee's email account and send a client a message stating that a payment has not come through and to instead send it to another account, which is in fact, the account pertaining to the perpetrator of the attack.
- A company lawyer impersonation, which involves attackers disguised as a company's lawyer and asking for money to pay for their services or a legal dispute.

Clone Phishing

Clone phishing consists of cyber attackers using a spoofed email address and taking an email with legitimate links sent from an official body and replicating it, but lacing the links within with malware before sending it to the victim.

These links lead the victim to a malicious website that could install malware onto a victim’s device, or steal personal information, such as login and bank details.

Snowshoeing

Snowshoeing involves senders utilizing an array of IP addresses and anonymous domains. This makes the emails more difficult for spam filters to detect, meaning that a proportion of them manage to enter inboxes.

The term originates from the snowshoe, the wearers of which use the footwear's large surface area to spread their weight and prevent themselves from falling into snow. The spam email-associated definition, however, relates to the spread of emails over several IP addresses.

The idea of snowshoeing spam is for it to be sent in small batches in order to decrease the likelihood of detection.

Cryptocurrency mining

Cryptocurrency mining, much like mining for silver, gold or other precious metals can be rewarding. However, the main purpose of cryptocurrency mining is to audit digital currency transactions and validate there is no double spending or duplicating digital certificates. Once you have validated a block of transactions, you must be the first to guess the correct answer to a mathematical problem called proof of work.

To do both validating and the proof of work, malicious actors create bot farms or mining camps by infecting 100’s or thousands of computers to use in the work effort, using CPU resources and bandwidth in the process.

What can be done to prevent these Cyber Attacks and Malware?

- Develop a strong Security Awareness Program to educate users on potential threats.
- The second webinar for this semester will address this issue:

Cybersecurity Tips and Tools – Establishing a Security Awareness Program

Mar 27, 2019 1:00 PM CDT

https://attendee.gotowebinar.com/register/4872991949290571266

The March 27th webinar provides information regarding establishing a Security Awareness Training program and what should be included in the program to make it beneficial to end users and your organization.

What can be done to prevent these Cyber Attacks and Malware?

- Implement Firewalls
- Spam filtering in multiple layers
- Implement endpoint security (anti-virus)
- Validate your backups
- Perform disaster recovery exercises
- Perform cyber-attack exercises

Questions?