SPRING BLOOMS CYBERTHREATS

A review of the latest security threats and how you can avoid them

THIS MONTH'S TOPICS:

External cybersecurity threats are at an all-time high. New scams and attacks are constantly emerging making an incident response plan a necessary piece of any organization's cybersecurity program.

While an incident response plan is a must for organizations to help them appropriately handle and recover from an incident, it can be extremely beneficial for individual use as well. We all face cyber-threats outside of the office too, so it's important we know what actions we'd take if an event were to happen to us.

Discover the critical components of a comprehensive incident response plan so you can spring into action when the moment arises.

Your Incident Response Plan

An incident response plan will help YOU navigate a cybersecurity incident if one were to occur outside of work. A good incident response plan will focus on 5 key areas: Preparation, Detection, Response, Recovery and Learning.

Preparation

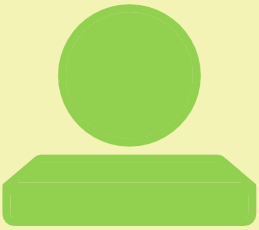
Failing to prepare is preparing to fail! Take some time to set your plan up for success by selecting an *incident response team* to help provide additional consultations. Also, make sure all your devices are backed up and protected with anti-virus/anti-malware protection.

Detection

Put your detective skills to work. Know some of the *warning signs* of an incident such as performance errors, inconsistent behavior, and system error messages.

Response

When it's time to take action, *respond quickly*! Don't panic and work with your team to find the best solution to the problem. Try shutting down your device and restarting it in "safe mode".



Recovery

When the dust settles after your incident, kick your *backup plan* into motion. Make sure the incident is fully resolved and work on recovering any lost data.

Learning

Share your knowledge and grow from your experience! Although it may seem embarrassing to admit that you've suffered an incident, your friends and family can benefit from learning how your incident occurred and what steps they can take to *better protect themselves*.

Just like any plan, make sure your incident response plan is tested. Of course, we aren't saying to purposefully infect your devices, but make sure the key elements of your plan are going to work as you expect them to and make sure the plan is understood by any other family members it may apply to.

Why Are Incident Response Plans *Important*?

Eliza tried to self-diagnose a problem on her device. She fell for an attack and didn't want to drag anyone else into her mess. Eliza made some crucial mistakes including calling a scammer's phone number that appeared on her device, then giving away her credit card information in an effort to fix the issue. If she had created and stuck to an incident response plan, Eliza could have worked with her incident response team to help resolve the situation correctly.

Bo was hit with ransomware on his laptop. He was able to contain then eliminate the malware but he failed to properly plan for an event like this. The ransomware encrypted his files and Bo did not have a recent backup of his information. Bo could have recovered from this event if he had followed the planning stage of an incident response plan to properly back up his devices.

Remember! Although it's important to create and follow an incident response plan for your own personal cybersecurity issues, if there is ANY issue affecting a work device, contact IT and your supervisor as soon as possible!

Celebrating Cybersecurity Heroes

https://www.darkreading.com/endpoint/intel-names-window-snyder-as-chief-software-security-officer/d/d-id/1332142

Window Snyder

Window is considered a pioneer for women in cybersecurity. Her passion for technology and security has led her to many prominent security positions at leading companies including Apple, Square, Microsoft, Intel, and Mozilla. She literally wrote the book on application security analysis, helping companies bolster their tools to keep our data safe.

https://womencybersecuritysociety.org/board-of-directors

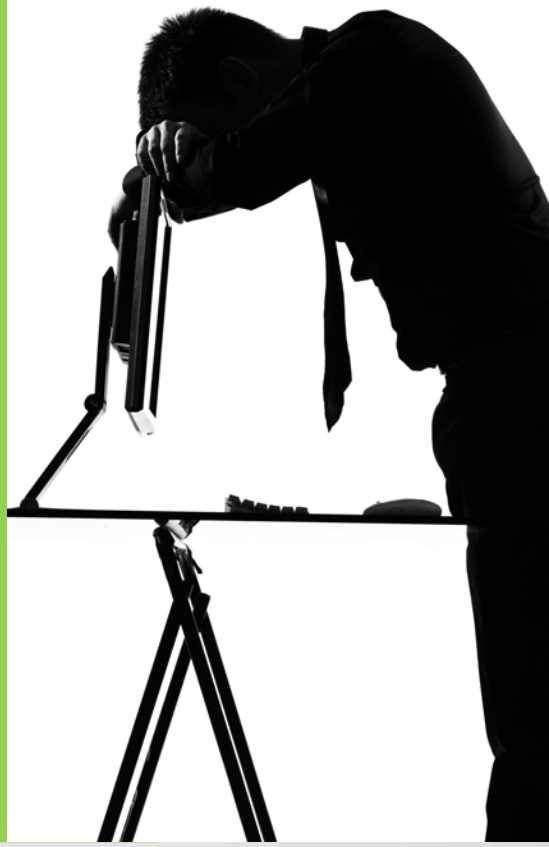
Lisa Kearney

Lisa has leveraged her decades of experience in the cybersecurity consulting arena to help kickstart her passion project. In 2018, Lisa founded the Women CyberSecurity Society (WCS2) in an effort to #recruit, #retrain and #retain women within the cybersecurity workforce. Through mentoring, training, workshops, scholarships, and more, the WSC2 is helping break down barriers and lowering the gender gap within the industry.

SCAM OF THE MONTH

Each month we highlight a REAL scam that was submitted to our security team. We highlight these real examples of tactics criminals are using RIGHT NOW, that way you'll be better prepared when the next scam hits.

Paulo doesn't know much about the tax process and generally fumbles through it. One day, Paulo received an email from his local tax agency with an important message about an error in his 2020 taxes. As this was one of his concerns, Paulo panicked and proceeded to open the attached Word document. The file that opened was blurred out and impossible to read but the text on the document read "Can't view the content? Please click "Enable Editing" and "Enable Content" on the yellow menu bar". As instructed, Paulo clicked these buttons. The blurred image did not improve but rather Paulo unleashed a powerful malware that took over his computer.



Did you spot the red flags?

- The supposed local tax agency sent Paulo an email with important tax information. Most reputable tax agencies will not use email to send or request sensitive tax material.
- The file Paulo opened had unreadable content, prompting him to "Enable Editing" and "Enable Content".

Enable Editing, Enable Content and Enable Macros are common tactics used in phishing campaigns. The scammer can easily design their malicious attack within a Macro. When their victim clicks on one of these prompts, they are allowing the malware to run, unleashing it onto the device.

This particular attack, when enabled, will release Remote Access Trojans, also known as RATs. When activated, the attacker can take control of their victim's device and steal sensitive information. Consistent with other attacks, these threats are designed to stay under-the-radar, making them more difficult to spot and stop by prevention tools.

This scam is very real and happening as we speak. Cybercriminals are able to purchase the tools to achieve these scams for a low price, and their purchase even includes a customer service support line! Watch for this or similar attacks this tax season and warn friends and family.

START PLANNING BEFORE IT'S TOO LATE!

Key Takeaways

Cybercriminals are successful when their targets are not prepared. Creating and following your incident response plan will help you win the fight against cybercrime.

Create your own incident response plan that can help you navigate security incidents outside of the office. Follow the steps of: Preparation, Detection, Response, Recovery, and Learning.

Test and be prepared to follow your incident response plan. Remember, if a cybersecurity event occurs on a work device, reach out to IT and your supervisor as soon as possible so they can handle the situation on their terms.

New tax scams are underway. Stay vigilant and know the warning signs. Never enable Content, Macros or Editing from an unsolicited sender. Inform friends and family so we all can be cyber-aware.

Cybersecurity Word Search

Can you find the cybersecurity words and phrases from this month's newsletter in the word search below?

Detection
Learning
Spring
Incident
Window
Tax Scam
Kearney
Recovery
Trojan
Macros

B P Y C G R A Y Y C N Z D P S
J T U E Z J R Y E Y T C T V Y
O P R P C E W B N C U L I C K
P K W L V T N T R E K U M P W
N A J O R T F S A K L X F H G
D H C X D D E T E C T I O N H
L E O E W N L G K F O I L M S
R W P P F U I E W U N E A Q P
M A C S X A T W A C Z C E C R
J O P E P K S H I R R U Q X I
Z U W Q B K L D P O N O R T N
Z G B S Y F E I S K L I Q T G
B C E G R N R P N B A N N Z N
R R O N T Q Q M Y B Q Y T G Z
I L W K C E Q A K M I C T Z P