ISSUE
12
October
2023

MONTHLY
TECH TIPS

TechTalk

this issue

This Month's Focus

Since 2004, the President of the United States and Congress have declared the month of October to be Cybersecurity Awareness Month.

This is the 20th Cybersecurity Awareness Month, and it has grown into a collaborative effort between government and industry to enhance cybersecurity awareness, encourage actions by the public to reduce online risk and generated discussion on cyber threats.

Securing the Human is a tough job for the IT team because there is no single learning technique that everyone will understand.

This newsletter is devoted to helping you understand how to

Scareware threats always seem perfectly timed!

Recently, a good friend of ours was in the middle of a transition, and they received a warning on their computer.

The warning said that their antivirus detected a hack of their computer.

Panic set in as they realized this attack could compromise their upcoming transition. They called the number provided and allowed them access to the computer to assist with the problem.

Once in the computer, it is hard to tell what trouble they caused.

These scary pop-ups or phone calls always seem to happen when we cannot be slowed down by technology. The panic overrides our ability to recognize false warnings and impairs our decision-making process.

Always check with a team member or your IT Department before allowing access or divulging any information. It's better to ask rather than be a victim!

Here are some points to review:

Ignore the pressure to make immediate decisions.

Look out for threats or harsh language; both are telltale signs of a scam.

Requests for money or financial account information are also huge warning signs.

Requests for personal or organizational information, including names and details of you or coworkers, are signs of someone gathering details for an attack.

Warnings of consequences such as fines or penalties.

Here are some tips on how team members should respond.

Hang Up

Report the call to your IT Department

Note details such as the time of the call and any specific information the caller provided.

Discuss the issue with a team member.

Make sure to share this information with your team and family!

ADVANCED
SYSTEMS SOLUTIONS

How to Determine Risks and Potential Business Impact.

Plan an effective response

A comprehensive business continuity plan will identify risks and develop an appropriate response to minimize or prevent them altogether.

Determine Roles and Responsibilities

In order for a crisis or disruption to be dealt with swiftly, the key people in your business need to know their roles and responsibilities.

Communication

Effective communication across your business can reassure team members and give them confidence that the organization is taking adequate steps to respond and recover.

Testing and training

Business continuity plans are not just theoretical; they need to be robust enough to be put into action. Schedule an attack simulation to see how quickly your organization can respond!

Simpson Manufacturing Victim of Cyberattack

Simpson Manufacturing disclosed via a SEC 8-K filing a cybersecurity incident that has caused disruptions in its operations.

Simpson Manufacturing is an American building and structural materials producer and one of North America's dominant makers of structural connectors with 5,150 employees and annual net sales of $2.12 billion.

Ransomware has disrupted critical services, businesses, and communities worldwide, and many of these incidents are perpetrated by actors using known common vulnerabilities and exposures.

However, many organizations may be unaware that a vulnerability used by ransomware threat actors is present on their network. To help organizations overcome this potential blind spot, vulnerability scans should be performed at least once a year or after significant changes to the

"The incident has caused, and is expected to continue to cause, disruption to parts of the Company's business operations." - Simpson Manufacturing

Also, the possibility of data theft would be a significant concern, as Simpson Manufacturing is a leader in its industry, potentially holding large amounts of proprietary information.

The firm operates seven laboratories for testing new designs and materials and holds over two thousand patents and trademarks.

However, the type of cybersecurity incident impacting Simpson Manufacturing has not yet been determined, and no ransomware groups have taken responsibility for an attack on the firm.

Here are some tips on how you should be prepared:

Encrypted Backups

An encrypted backup is a backup that protects data by using encryption algorithms to maintain the authenticity, confidentiality, and integrity of information as well as prevent unauthorized access.

Business Continuity Plan

This plan decreases business downtime and outlines the steps to be taken before, during, and after an emergency to maintain the company's financial viability.

How Do you Recover from an Attack?

Contact your IT Team immediately. Then contact the institution of any account information you might have shared. Review your processes and procedures to keep it from happening again.

Details Here

Areas for Review This Month

We recommend that you take this month to review your habits.

Use Strong Passwords:

Strong passwords are long, random, and unique. They include all four character types (uppercase, lowercase, numbers, and symbols).

Password generators are a powerful tool to help you create strong passwords for each of your accounts. Try https://www.random.org/passwords/ as a tool to help create a strong password.

Also, your banking passwords should not be

Turn On MFA:

You need more than a password to protect your online accounts and enabling MFA makes you significantly less likely to get hacked. Enable MFA on all your online accounts that offer it, especially email, social media, and financial accounts.

Recognize & Report Phishing:

Be cautious of unsolicited messages asking for personal information. Avoid sharing sensitive information or credentials with unknown sources. Report phishing attempts and delete the message. **TIP** - When creating password hints, use fake information!

Remove Unused Software:

Many people load software such as "Zoom" or "GoToMeeting" but never return to uninstall the service. Then, when updates are released, the software doesn't get updated if it is not used.

Help Your Family and Friends:

Our world is increasingly digital and increasingly interconnected. So, while we must protect ourselves, we will all need to protect the systems we rely on.

Being cyber-smart is contagious. Take the four basic steps above and help two friends or family members do the same!

This Month's Q&A Technology Tips

Q: Kim from Kansas asks, "My brother's social media account was hacked, and they are asking family members for money. How can he regain access to his account?"

A: It is a sad truth, but when a social media account is hacked, the support team for that organization is usually very slow to respond. Each platform has a different set of hoops to jump through and we have found that the typical time to regain access to your account is four to six weeks. This is why it is critical to accounts with two-factor authentication (2FA). Once it is configured, you can remember the device you always use. This will make sure any new access from an unknown device will prompt for the authentication. Microsoft reports that using 2FA will decrease the possibility of an account breach by 99.9%. This will stop imposters from preying on your family and friends asking for help!

We suggest contacting people who may be easy prey and assuring them that your brother is okay.

Thanks for the question, Kim. We hope this helps!

Have a question?

Ask us at - info@advancedsystemssolutions.com

Fourteen Phrases We Should All Know:

Here are fourteen phrases everyone should know:

Ransomware

Malware

You Are The Shield

Social Engineering

Phishing

Smishing

Vishing

Passwords

Multifactor Authentication

CEO Fraud

Data Protection and Loss

Social Networks

Mobile Devices

Remote Access

If you would like help making sure that your team members are aware of above areas, call us and we will help your team understand that they are the first line of defense!

(Click here for details - https://bit.ly/14phrases)

Stay Up to Date!

Don't forget to check out our additional tips to keep you secure! If you are not familiar with the tips and tricks to stay secure, you will want to check out our posts to keep your organization secure.

https://bit.ly/ASSI_Blog

Upcoming Events

- ### FLGISA 2024 Winter Symposium

  The 2024 Winter Symposium is scheduled for January 30-February 1, 2024, at the Embassy Suites Lake Buena Vista South. Registration details will be available in November. We look forward to seeing you there!

  https://www.flgisa.org/events/

- ### Small Business Expo

  It is a few months, but if you are unaware of Orlando's biggest business networking & educational event for Small Business Owners & Entrepreneurs, you must plan to be there! It is the perfect event for business owners to see new solutions to small business problems.   March 21, 2024 10:00 AM-5:00 PM

  https://www.thesmallbusinessexpo.com/city/orlando/

- ### Orlando Power Lunch

  The Orlando Power Lunch will be held on November 2nd. The location has not been determined, so follow them on Facebook!
  https://www.facebook.com/OrlandoPowerLunch
  https://www.orlandopowerlunch.com

You will not want to miss these events!

ADVANCED SYSTEMS SOLUTIONS

6965 Piazza Grande Ave 210-1
Orlando, FL 32835
407-414-6626
www.advancedsystemssolutions.com