ISSUE
10
October
2021

MONTHLY
TECH TIPS

TechTalk

this issue

This Month's Focus

When it comes to securing the network, IT engineers typically recommend the same basic principles for protecting the infrastructure. These include a firewall, a DMZ (demilitarized zone) segmentation, and so on.

Cybercriminals are very aware of the tools that the IT engineers use and know how to circumvent everything in under an hour, and no software or hardware can protect us from it. How do they do it? They use the telephone.

Securing the Human is one of that toughest jobs for the IT team because there is no single way that people learn.

Vishing is the term for this cyberattack, and we discuss it on page two this month.

October Is Cybersecurity Awareness Month

Celebrating the 18th Year of Working to keep America Secure.

Cybersecurity Awareness Month was launched by the National Cyber Security Alliance and the U.S. Department of Homeland Security (DHS) in October of 2004 as a broad effort to help all Americans boost their cybersecurity awareness.

In the Beginning:

When Cybersecurity Awareness Month began, the message was focused on updating antivirus software twice a year to mirror the message of changing batteries in smoke alarms during daylight saving time. Ironically, Fire Prevention week also takes place in October

In 2021:

This year's initiative is led by the National Cyber Security Alliance (NCSA), in partnership with the Cybersecurity and Infrastructure Security Agency (CISA) to ensure that everyone has the resources they need to be safer and more secure online. This year's theme for the month-long campaign is "Do Your Part. #BeCyberSmart." which encourages individuals and organizations to own their role in cybersecurity. The message stresses personal accountability and the importance of proactive steps to increase security.

Today's Climate:

"We've seen an unprecedented shift to more digital usage in the last year and there's no going back," said Lisa Plaggemier, Interim Executive Director, NCSA. "The onset of the ongoing pandemic and the need to stay connected has made our digital life prone to cyber threats now more than ever.

Advanced Systems Solutions Inc.

What Does the CISA Do?

The Cybersecurity and Infrastructure Security Agency, CISA, is responsible for protecting the Nation's critical infrastructure from physical and cyber threats. This mission requires effective coordination and collaboration among a broad spectrum of government and private sector organizations.

CISA Releases Telework Guidance and Resources

(click here for details)

CISA's National Cybersecurity and Communications Integration Center provides 24x7 cyber situational awareness, analysis, incident response and cyber defense capabilities to the Federal government; state, local, tribal and territorial governments; the private sector and international partners.

CISA Issues Warnings Regarding Vishing Threat

"Cyber Criminals Take Advantage of Increased Telework Through Vishing Campaign" warns the FBI and CISA.

Voice phishing, or vishing, is the use of the telephone to conduct phishing attacks.

Voice Phishing comes in many formats but for this month's example we are going to keep it basic.

Through voice communication, vishing attacks can be personable and therefore more impactful than similar alternatives such as email. In addition, there is no firewall or other electronic means to determine the validity of the call. Therefore, it is important that team members stay alert.

When a provider says they are unable to service the area, residents are usually under the impression it is the fault of government, but it is the providers who are to blame.

It Is Critical That We Teach Team Members How To Catch A Vish

It is important to review with your team that Microsoft will never call and ask for their password.

Here are some other areas to review:

Offers from companies you do not do business with and/or have not heard of.

Assistance in resetting a password.

Ignore pressure to make immediate decisions that give the caller what they want such as threats or harsh language.

Requests for money or financial account information.

Requests for personal or organizational information, including names and details of you or coworkers.

Threats of consequences such as fines or penalties.

Here are some tips on how team members should respond.

Hang Up

If they will not provide a callback number or will not let you end the call, disconnect the call and call the organization back using a known valid phone number. If it was a scam, REPORT IT!

Do Not Press Buttons

Automated vishing calls depend on feedback from the victim. If you don't press buttons or answer questions, the attack can be stopped.

How Do you Recover from a Vishing Attack?

Contact your IT Team immediately. Then contact the institution of any account information you might have shared. Perform a review of 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 team.

Securing The Human: Building and Maintaining a Cybersecurity Awareness Program.

Organizations invest a tremendous amount of money and resources into securing technology, but little if anything into securing the human. As a result, people, not technology, have become the most recent target for cyber criminals. The most effective way to secure the human element is to establish a high-impact security awareness program that goes beyond compliance and change behaviors and ultimately creates a secure culture.

Every Role Is Different.

Identify and prioritize the top human risks to your organization and the key behaviors that manage those risks. The reception team will need more focused attention than the landscape team.

Engage your team while considering the challenges of different roles, generations, and nationalities. Everyone learns at a different pace, so make sure that your cybersecurity training caters to your team's needs.

Keep conversations brief as many become bored when it comes to talking about IT security.

Sustain your security awareness program long term.

Keep the topics of discussion brief, but frequent. This is a marathon, not a sprint. Talking about security briefly once a month is better than for a long time once a year.

Measure the impact of your awareness program, track reduction in human risk, and communicate the value to leadership.

Most importantly, monitor your team member's progress. Their awareness is better than any firewall.

This Month's Q&A Technology Tips

Q: Katey from Kensington asks, "Given that October is Cybersecurity Awareness Month, what is the best thing I can do to make sure that my online accounts are safe?"

A: Awesome question Katey, thanks for asking! Two-factor authentication, or 2FA, reduces the chance of an account breach by 99%. About a year ago, Alex Weinert from Microsoft wrote an article that had some great points. Weinert said that old advice like "never use a password that has ever been seen in a breach" "use really long passwords" doesn't really help.

He attributed this to the fact that passwords or their complexity don't really matter anymore. Nowadays, hackers have different methods at their disposal to get their hands on users' credentials, and in most cases, the password doesn't matter.

Weinert says that enabling a multi-factor authentication solution will block 99.9% of unauthorized login attempts, even if hackers have a copy of a user's current password.

Thanks again for the question Katey, I hope this helps!

Have a question?

Ask us at - info@advancedsystemssolutions.com

Fourteen Phrases Your Team Should All Know

Here are fourteen phrases everyone in your organization 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 new features in Edge, you will want to check out our guidelines for keeping your organization secure.

https://bit.ly/ASSI_Blog

Upcoming Events

- **FLGISA 2021 Winter Symposium**

  The 2022 Winter Symposium is scheduled for January 25-27 at the Embassy Suites Lake Buena Vista South. Details and registration will be available in November 2021. We look forward to seeing you there!

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

- **T2 Tech Talk Podcast**

  We know tech and marketing can be daunting, but we break it down into byte sized chunks.

  https://www.t2techtalkpodcast.com/

- **Orlando Power Lunch**

  In May, The Orlando Power Lunch is proud to feature Sherry R. Gutch, the Business Development Division Manager in the Economic Development Department at Orlando

  https://www.orlandopowerlunch.com

You will not want to miss these events!

Advanced Systems Solutions Inc.

1051 Winderley Place #307
Maitland, FL 32751
407-414-6626
www.advancedsystemssolutions.com