ISSUE
11
March
2022

MONTHLY
TECH TIPS

TechTalk

This Month's Focus

Cybersecurity starts with you!

When it comes to securing workstations, IT staff typically recommends the same principles. These include performing updates, strong passwords, and an offline backup.

Cybercriminals work extremely hard to exploit vulnerabilities quickly, prior to updates provided by software vendors and before you install the patch.

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 keep you, and your data, protected!

this issue

Turn on Multi-Factor Authentication (MFA) Now!

Implement multi-factor authentication on your accounts and make it 99% less likely you'll get hacked.

The Cybersecurity & Infrastructure Security Agency (CISA) and Microsoft both agree that securing accounts with MFA will decrease your chances of a data breach by 99%.

What is MFA:

When you enable MFA in your online services (like email), you must provide a combination of two or more authenticators to verify your identity before the service grants you access. Using MFA protects your account more than just using a username and password.

Because even if one factor (like your password) becomes compromised, unauthorized users will be unable to meet the second authentication requirement ultimately stopping them from gaining access to your accounts.

Prove It's You With Two:

Use a combination of something you have, something you know, or something you are when confirming you are who you say you are online.

Your bank, your social media network, your school, your workplace all want to make sure you're the one accessing your information. More importantly, they want to prevent unauthorized individuals from accessing your account and data.

Now that you know what it is, you'll notice prompts to use multi-factor authentication. Whenever available - opt-in! Start with your email account, then financial services, then social media accounts, then online services.

Two steps are harder for a hacker to compromise. So, prove it's you with two. Two steps, that is!

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.

Avoid Social Engineering and Phishing Attacks

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

Phishing is a form of social engineering. Phishing attacks use email or malicious websites to solicit personal information by posing as a trustworthy organization.

An attacker may send an email that appears to be from a reputable credit card company or financial institution that requests account information, often suggesting that there is a problem. When users respond with the requested information, attackers can use it to access the accounts.

Phishing attacks may also appear to come from other types of organizations, such as charities. Attackers often take advantage of current events and certain times of the year, such as the conflict in Ukraine, Holiday deliveries, politics, or natural disasters.

NEVER Provide Details In Response to Unsolicited Calls, Visits, or Email Messages.

Most organizations will never send you a request to provide, verify, or update your personal information.

If unknown individual claims to be from a legitimate organization, try to verify their identity directly with the company.

Here are some other thoughts to review:

Ignore the 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 an 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

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

Fix known security flaws in software:

There are many instances where software will not be upgraded because the current version is still working.

Just because the software still works doesn't mean that it is safe to use. Many vendors provide guidelines for support throughout the lifecycle of a product, helping you to manage your investments and strategically plan for the future.

Areas for Review This Month

Think Before You Click:

Have you ever seen a link that looks a little off?

It looks like something you've seen before, but it says you need to change or enter a password. Or maybe it asks you to verify personal information.

It could be a text message or email. They may pretend to be your vendor, your boss, your bank, a friend, etc.

The message may claim it needs your information because you've been a victim of cybercrime.

If it's a link you don't recognize, trust your instincts and think before you click. We all need to Phight the Phish!

Help Your Family and Friends:

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

Being cyber smart is contagious. Take the four basic steps outlined above and help two friends do the same.

Remove Unused Software:

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

This Month's Q&A Technology Tips

Q: Caleb from Cape Canaveral asks, "What is the best thing I can do to make sure that my data is protected?"

A: It is a sad truth but firewalls and antivirus solutions aren't enough to completely protect our data anymore. When creating your data backup plan, follow the 3-2-1 rule. The 3-2-1 backup rule means that you should:

- Have at least three copies of your data.
- Store the copies on two different media.
- Keep one backup copy offsite.

it is important to test your data recovery plan at least once every few months. All too often people assume that the data is being backed up but when they try to recover the data, they discover that it was not working as intended. To test, check to make sure that you can restore a file or two.

The only protection against ransomware is a solid data recovery plan. Create a data recovery plan or plan to lose your data, the choice is yours.

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

Have a question?

Ask us at - info@advancedsystemssolutions.com

Fourteen Phrases You 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 new features in Edge, you will want to check out our guidelines for keeping your organization secure.

https://bit.ly/ASSI_Blog

Upcoming Events

- **NAWIC Southeast Region Forum 2022**

  The 2022 NAWIC Southeast Region Forum is scheduled for April 29-30 at the DoubleTree by Hilton Universal. Details and registration are both available online. We look forward to seeing you there!

  https://www.nawicsoutheastregion.org/forum-2022

- **Small Business Expo**

  Orlando's biggest business networking & educational event for Small Business Owners & Entrepreneurs. March 16, 2022

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

- **Orlando Power Lunch**

  The April Orlando Power Lunch will be held at the Advanced Systems Solutions Inc. headquarters in Maitland Florida.

  https://www.orlandopowerlunch.com

You will not want to miss these events!

Tech Talk Issue 11 March 2022

Advanced Systems Solutions Inc.

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