BSSi2

Innovations

Review Twice, Implement Once. Doing IT Right the First Time.

Don't Let Your Employees Become Your Biggest Vulnerability

A couple years ago, TechRepublic ran a story with the following headline: "Employees Are Almost As Dangerous To Business As Hackers And Cybercriminals." From the perspective of the business, you might think that's simply inaccurate. Your company strives to hire the best people it can find – people who are good at their jobs and would never dream of putting their own employer at risk.

And yet, many employees do, and it's almost always unintentional. Your employees aren't thinking of ways to compromise your network or trying to put malware or ransomware on company computers, but it happens. One Kaspersky study found that 52% of businesses recognize that their employees are "their biggest weakness in IT security."

Where does this weakness come from? It stems from several different things and varies from business to business, but a big chunk of it comes down to employee behavior.

Human Error

We all make mistakes. Unfortunately, some mistakes can have serious consequences. Here's an example: an employee receives an e-mail from their boss. The boss wants the employee to buy several gift cards and then send the gift card codes to them as soon as possible. The message may say, "I trust you with this," and work to build urgency within the employee.

The problem is that it's fake. A scammer is using an e-mail address similar to what the manager, supervisor or other company leader might use. It's a phishing scam, and it works. While it doesn't necessarily compromise your IT security internally, it showcases gaps in employee knowledge.

Another common example, also through e-mail, is for cybercriminals to send files or links that install malware on company computers. The criminals once again disguise the e-mail as a legitimate message from someone within the company, a vendor, a bank or another company the employee may be familiar with.

It's that familiarity that can trip up employees. All criminals have to do is add a sense of urgency, and the employee may click the link without giving more thought.

Carelessness

This happens when an employee clicks a link without thinking. It could be because the employee doesn't have training to identify fraudulent e-mails or the company might not have a comprehensive IT security policy in place.

Continued on the next page...

Continued from previous page...

Another form of carelessness is unsafe browsing habits. When employees browse the web, whether it's for research or anything related to their job or for personal use, they should always do so in the safest way possible. Tell employees to avoid navigating to "bad" websites and to not click any link they can't verify (such as ads).

Bad websites are fairly subjective, but one thing any web user should look for is "https" at the beginning of any web address. The "s" tells you the site is secure. If that "s" is not there, the website lacks proper security. If you input sensitive data into that website, such as your name, e-mail address, contact information or financial information, you cannot verify the security of that information and it may end up in the hands of cybercriminals.

Another example of carelessness is poor password management. It's common for people to use simple passwords and to use the same passwords across multiple websites. If your employees are doing this, it can put your business at a huge risk. If hackers get ahold of any of those passwords, who knows what they might be able to access. A strict password policy is a must for every business.

Turn Weakness Into Strength

The best way to overcome the human weakness in your IT security is education. An IT security policy is a good start, but it must be enforced and understood. Employees need to know what behaviors are unacceptable, but they also need to be aware of the threats that exist. They need resources they can count on as threats arise so they may be dealt with properly. Working with an MSP or IT services firm may be the answer – they can help you lay the foundation to turn this weakness into a strength.

Business Tidbit

Retain Top Talent By Teaching Them To Grow

Throughout the course of 2021, Americans left their jobs in droves due to a combination of factors. In fact, an analytics firm, Visier, estimates that 1 out of 4 workers left their jobs in 2021. If you own or operate a business, this news can be worrisome. One of the best ways to try to retain your employees is to coach and encourage them to grow so they don't feel stagnant and bored with their work.

If you don't know where to begin, you should start by evaluating your employees. Decide if they're a master in their role, are still growing or are just beginning. Keep an eye on your beginners and growers to ensure they are satisfied with their work. If they're not, have an open and honest discussion with them. For employees who have mastered their jobs, encourage them to try a new role or take on different responsibilities so they can learn new skills.

On the Lighter Side

April Fools' Day is like a huge open mic night.
Millions of people go out of their way to demonstrate how unfunny they are.

A and C were going to prank their friend…
But they just letter B.

A couple of pranksters broke into the local police station and stole all the lavatory equipment.
A spokesperson was quoted as saying "We have absolutely nothing to go on."

Carrie's birthday is in April, which is in the fall. How is this possible?
Carrie lives in Australia.

What 5-letter word becomes shorter when you add two letters to it?
"Short"

When written forward, this word is heavy. When written backward, it is not. What word is this?
Ton

Do You Know Which Documents to Keep and Which Ones to Shred?

By John Klise from Paper Tiger

It's almost tax time. For many individuals and organizations, that means it's also time to clean your office or home and purge. But do you know which documents are important to retain and which ones you should (or can) shred? Some guidelines are below. (For more information please contact your accountant or attorney.)

Documents to Keep Forever

- Social Security Cards
- Death Certificates
- Legal Filings
- Beneficiary Forms
- Immunization Records
- Marriage Certificates
- Passports
- Military Records
- Powers of Attorney
- Birth Certificates
- Adoption Papers
- Wills/Living Wills
- Inheritance Document
- Retirement Plans

Keep these documents while they are active/current:

- Contracts
- Property Records
- Stock Certificates
- Product Warranties
- Stock Records
- Insurance Documents
- Disputed Bills

Keep these up to 1 year:

- Pay Stubs
- Bank Statements
- Credit Card Statements
- Investment Statements
- Medical Bills
- Receipts for Large Purchases

Keep these for 3-5 Years:

- Title Insurance Policy
- Deeds/Mortgages
- Home Improvement Records

Keep these for 7+ Years:

- Tax Records
- W-2 Forms
- 1099 Forms

We've updated our website. Make sure to check it out!
www.bssi2.com

April 2022

35 Aztec Court
South Barrington, IL 60010
(312) 752-4679
www.bssi2.com

"We make all of your computer problems go away without the cost of a full-time I.T. staff"

Shiny New Gadget of the Month

Garmin Venu 2 Plus Smartwatch

One of Garmin's newest smartwatches is setting the standard for the industry. The Garmin Venu 2 Plus smartwatch comes in three different sizes and in various colors. With the Venu 2 Plus, you can connect the smartwatch to your mobile device, make phone calls and send text messages – all hands-free. The best functions of this smartwatch all relate to health and wellness since it gives you greater insight into your stress, hydration and respiratory levels. It can also keep track of your sleep patterns, heart rate and so much more. The smartwatch holds nine days of battery life, so it's perfect for backpackers and hikers. If you're looking for a great smartwatch, look no further than the Garmin Venu 2 Plus.

Stay up-to-date

Follow BSSi2 at:

www.facebook.com/bssi2

twitter.com/BSSi2llc

"Obviously, we need to readjust to in-office meetings."

CartoonStock.com