

# TECHNOLOGY TODAY

## EASY PICKIN'S

Passwords are easy to crack using software tools like Aircrack, Hashcat, Hydra, John the Ripper or Cain and Abel. Then there are Phishing attacks designed to get the user to reveal it themselves. Simply put, if Cyber crooks want a password, there are a number of ways they can get it.

Your password by itself is like using a chain-link fence for protection. You want a Castle Wall. Couple strong passwords with Multi-Factor Authentication. One secondary level are questions like 'Your mother's maiden name'. Another level is a body part - thumbprint, retinal scan etc.

The first step to keeping your system secure is to create the strongest possible passwords.

Get great advice here:  
[www.itsupportla.com/creating-strong-passwords/](http://www.itsupportla.com/creating-strong-passwords/)

## October 2020



This monthly publication provided courtesy of Yuri Aberfeld, CEO of IT Support LA.

Our vision is to pioneer a paradigm shift in the IT industry by redefining the customer experience through effective communication and positive interaction.



## The #1 Mistake Your Employees Are Making Today That Lets Cybercriminals Into Your Network

We all make mistakes. It's a fact of life. But as we all know, some mistakes can have serious and lasting consequences - especially when it comes to business, cyber security and the constant cyberthreats that are out there.

While some businesses have invested heavily in cyber security, many have not. When it comes to network and data security, one of the most vulnerable areas of the economy is small businesses.

More often than not, small businesses simply don't go all-in when it comes to IT security. Some fear they don't have the budget and worry that IT security is too expensive. Others don't take it seriously - they have an "it will never happen to me" attitude. Then there are those who invest in *some* security, but it's limited and still leaves them vulnerable in the long run.

But there is one area of IT security where *every* business is vulnerable. You can have the greatest malware protection in the world and still fall victim due to this one big mistake.

### Your employees lack IT security training.

It's as simple as that. When your team isn't trained on IT or network security *and* they aren't aware of today's best practices, you open yourself to major risk. Here's why: We make mistakes.

Scammers and cybercriminals have the most success when they are able to trick people or play on the emotions of their victims. One common emotion they use is fear.

No one likes to get a message telling them that their bank account has been compromised. This is how phishing e-

Continued from pg.1

mails work. The scammer sends an e-mail disguised as a message from a bank or financial institution. They may tell your employee that their account has been hacked or their password needs to be changed immediately. They use fear to trick them into clicking the link in the e-mail.

So, concerned about their bank account, your employee clicks the link. It takes them to a web page where they can enter their username, password and other credentials. Sometimes it even asks for their full Social Security number. (Scammers are bold, but people fall for it!)

As you guessed, the web page is fake. The link in the e-mail directs your employee to a page that allows the scammer to collect their data. Some thieves use it to access their bank account, but others sell the information for a quick buck. No matter the situation, the information has fallen into the hands of crooks.

The challenge is that phishing e-mails have gotten harder to spot. Scammers can spoof legitimate web addresses. They can make fake e-mails look like the real deal. But there are still plenty of minor details that indicate the e-mail is a fake.

This is one of the MANY reasons why comprehensive employee IT training is so important. Training helps employees identify red flags. But more than that, it helps them identify *changing* red flags. For instance, a phishing e-mail from 2010 looks nothing like a phishing e-mail from 2020.

**“Your employees are your first defense against outside cyber-attackers.”**

Scammers stay ahead of the curve. They know the trends, and they know how to adapt. Your employees also need to know the trends and need to be ready to adapt.

Good IT training covers much more than phishing e-mails. It helps your employees identify security red flags across the board.

These include:

- Phishing e-mails and phone calls
- Poor or outdated passwords
- Malicious software hidden in links, attachments or online ads
- Poorly configured security on employee devices (a big deal for remote employees!)
- Lack of guidelines related to Internet or social media usage on employee devices
- Outdated software or hardware

Good training is also continuous. Cyber security training isn't a one-and-done deal. It's something you do every quarter or twice a year. Just as you keep your business's equipment maintained, you have to keep your employees' cyber security knowledge maintained. After all, your employees are your first defense against outside cyber-attackers. When they know what they're dealing with, they're better equipped to stop it in its tracks and protect your business.

The bottom line is that a lack of training is the biggest threat against your computer network and the health of your business. You need to have a strong training program in place to make sure your employees stay up-to-date. But you don't have to do it yourself. We can help. Along with your team, let's protect your business together.

## Free Report Download: If You Are Considering Cloud Computing For Your Company, DON'T, Until You Read This...

### INTRO TO CLOUD COMPUTING

“5 Critical Facts Every Business Owner Must Know Before Moving Their Network To The Cloud”



Discover What Most IT Consultants Don't Know Or Won't Tell You About Moving Your Company's Network To The Cloud

If you are considering cloud computing or Office 365 to save money and simplify IT, it is extremely important that you get and read this special report: “5 Critical Facts Every Business Owner Must Know Before Moving Their Network To The Cloud.”

This report discusses in simple, nontechnical terms the pros and cons of cloud computing, data security, how to choose a cloud provider and three little-known facts that most IT consultants don't know or won't tell you about cloud computing that could end up causing you MORE problems and costing you more money than you anticipated. **Even if you aren't ready to move to the cloud yet**, this report will give you the right information and questions to ask when the time comes.

Get your FREE copy today:

[www.itsupport.com/cloudreport/](http://www.itsupport.com/cloudreport/)

Get More Free Tips, Tools and Services At Our Website: [www.itsupportla.com](http://www.itsupportla.com)  
(818) 805-0909

## Do Not PAY Them!

Cyber Criminals still count on most companies being ill-prepared for a Ransomware or Hack-attack. The sad news is that they are right. They are not worried about Small and Mid-size Businesses (SMBs) putting up viable defense, and they are not worried about firms that promise High-Tech solutions to an attack. The sad fact is, many of these 'Heroes' riding to the rescue are just paying the hackers and charging their clients extra for their own pocket. SMBs could pay the ransom themselves and save some cash on the fraudulent 'middleman'.

Another sad fact is that it is hard to catch these fraudsters. So as the CEO of an SMB, what is there to do?

### Do Not Pay THEM, Either!

*Statistics show that, over the last 5 years, 33% to 40% of companies that PAID the Ransom to have their data de-crypted and returned, DID NOT get their data restored. Over 60% of businesses that lost access to their customer data for longer than TWO WEEKS did not survive.*

**What to Do:** This is not Rocket Science. On the elemental level, Ransomware can be quickly remedied with solid local backups to a Dedicated Storage unit that is NOT connected to the main network. This ensures fast restoration of data once your affected workstations and server have been wiped clean. Further backup to the Cloud is essential.

That is it in a nutshell, but there's more to it. We offer a **FREE** Network/Cyber Security Audit that will show you where your weak spots are and how to 'bullet-proof' them.

Call us at **818-805-0909** or visit:  
[www.itsupportla.com/free-stuff/free-network-security-assessment/](http://www.itsupportla.com/free-stuff/free-network-security-assessment/)

## What Makes A Leader Successful Today? *Intentionality And The 3 Shifts*

Have you ever wondered what one thing all successful leaders have in common? First, consider what all *unsuccessful leaders* have in common: they lack focus.

Either they aren't clear on what they're trying to do or they know what they need to do but aren't doing the right things to achieve their objectives. Both waste money and resources and leave organizations stuck in the status quo.

This affects leaders regardless of the size or type of organization, and that's why I wrote *The Intention Imperative: 3 Essential Changes That Will Make You A Successful Leader Today*.

What all great leaders have in common is intentionality — *being crystal clear on what you're trying to achieve and taking the right actions every day to achieve it.*

Why do many business leaders lack clarity?

1. They inherited an unclear vision or never had one to begin with.
2. They value operations over objectives — doing things without questioning why.
3. They were distracted by problems, or even opportunities, which took them off course.
4. They were unwilling or unable to look at what was consistently being done with a fresh perspective.

What are the symptoms and signs of a leader who lacks clarity?

1. Constant changes in focus or direction
2. Lack of momentum
3. Confusion among employees and what to do
4. Many team members asking "Why?"
5. Frustration at every level
6. Inconsistent action or behavior

In my book, I explain intentionality and then share what I believe are imperative changes

leaders need to take today to succeed: the shift from *structure to culture*, from *motivation to inspiration* and from *experience to emotion*.

### IMPERATIVE 1 - CULTURE

*"Culture is what we think and believe, which then determines what we do and what we accomplish."*

In *The Intention Imperative*, I teach the five levers you have for creating and maintaining the culture you desire. Creating it is the job of a leader.

### IMPERATIVE 2 - INSPIRATION

*"Inspiration doesn't have to be mysterious or complicated to create."*

What is inspiration? It is motivation to the power of purpose. It is linking meaning to motives. Inspiration doesn't come from outside force or artificial causes. It develops from the work itself and how the leader is able to demonstrate importance and impact.

### IMPERATIVE 3 - EMOTION

*"Emotions are everywhere and they are the single biggest factor in how we make decisions."*

A negative emotional experience can be offset with a positive one. The customer experience is important, but how the customer feels about that experience is critical. Few companies design and deliver for positive emotion.

*Now, try these three things:*

1. Focus on building a culture that powers the right actions to create the right results you, your team and customers need for breakthrough success.
2. Couple purpose with motivation so your team is inspired.
3. Design your product and service delivery around positive emotions.



*Mark Sanborn, CSP, CPAE, is the president of Sanborn & Associates, Inc., an "idea studio" that seeks to motivate and develop leaders in and outside of business. He's the best-selling author of books like Fred Factor and The Potential Principle and a noted expert on leadership, team building, customer service and company change. He holds the Certified Speaking Professional designation from the National Speakers Association and is a member of the Speaker Hall of Fame. Check out any of his excellent books, his video series "Team Building: How To Motivate And Manage People" or his website, [MarkSanborn.com](http://MarkSanborn.com), to learn more.*



## ■ Improve Your Cash Flow With These Tips

### Have Better Billing Processes –

Make it as easy as possible for customers to pay their bills. Incentivize them to pay before the due date with a small discount or offer. Be diligent about sending invoices ASAP after customers buy with you.

### Get Cooperative –

If it's possible or practical, work with other businesses to form a buyers' co-op. This gives you more buying power when buying in bulk.

### Credit Check Customers –

When dealing with higher-priced goods or services and a customer can't pay in cash, don't be afraid to run a credit check. Customers with poor credit can be a liability and cost you big.

**Audit Your Inventory** – Identify what costs you money by sitting around. If you're stuck with inventory that isn't moving, you

may need to discount it to get rid of it.

**Pay Online** – Pay all of your bills online. This way you can select the exact date when those bills are paid each month, giving you more control over your cash flow.

*SmallBiz Technology, Jan. 27, 2020*

## ■ Top Ways To Prevent Your Remote Workers From Letting Cybercriminals Steal Your Data

1. Set expectations, rules and boundaries for employees, ensuring everyone is on the same page and held accountable.

2. Put together standard operating procedures for employees so they know what to do and who to call should anything go wrong.

3. Have a disaster recovery plan ready to back up and restore any system or data, should it become compromised.

4. Establish guidelines for employees, defining which approved devices and software they should be using.

5. Make sure those devices and software are routinely updated with the latest security patches.  
*Cyber Defense Magazine, June 3, 2020*

## ■ 3 Things You Can Do To Use Stress To Your Advantage

**Embrace Deadlines** – Research suggests we are the most productive with deadlines looming. Give yourself deadlines for everything. If you struggle with procrastination, move deadlines up in order to get things done.

### Stress Yourself Out (On Purpose)

– You can actually build a tolerance to stress. All you have to do is step out of your comfort zone and intentionally put yourself into stressful situations. You become more resilient to stressful situations and test your own boundaries at the same time.

### Identify Stress “Weaknesses” –

When stressed, identify what it is about a situation or task that is causing you stress. Then, focus on that cause and determine what you can do to mitigate it. It might mean reorganizing your day, such as reading and responding to e-mails at a different time. Or maybe you need more information on the issue you're dealing with, so do some research and see what you can find to help.  
*Inc., July 8, 2020*



"But I think we can both agree that my nap ethic is fantastic."