Cyber Security Best Practices

By: Eric Kehmeier

Integrated Business Technologies
1800 South Elm Pl., Suite 200 / Broken Arrow, OK
918.770.8738 / www.IBTsupport.com

COMPANY PROFILE

Since 2007, Integrated Business Technologies (IBT) has helped small and medium-sized businesses in Oklahoma align their technology needs with their business goals. Our experience has allowed us to build and develop the infrastructure needed to provide enterprise-level IT support and solutions at an affordable price. We work as an extension of your team, enabling you to focus on growing your business.

- INC. 500|5000 (2012, 2013, 2014, 2015)
- MSPmentor 501 Global – Top 501 Managed Service Providers (2012, 2013, 2014)
- DELL SMB Partner of the Year for the US (2012)
- BBB Excellence in Customer Service (2009, 2010, 2011, 2012, 2013, 2014)
- Tulsa's Fast 40 (2011, 2012, 2013, 2014)
- Employees Choice Award – Tulsa's Best Places to Work (2011, 2012, 2013, 2014)
- okcBIZ – Best Places to Work in Oklahoma (2012, 2013, 2014, 2015)
- CRN – Next Gen 250 (2012, 2013)
- CRN – Fast Growth 150 (2013, 2014, 2016)
- CRN – MSP500 - Pioneer 250 (2017, 2018)

IBT

DID YOU KNOW?

The last five years have shown a steady increase in attacks targeting businesses with less than 250 employees. [1]

Nearly 59% of U.S. small and medium sized businesses do not have a contingency plan that outlines procedures for responding to and reporting data breach losses. [2]

The primary cause of security breaches is typically human error (58 percent) versus technology error (42 percent). [4]

More than 75% of employees leave their computers unsecured. [3]

60% of small business will close within six months of a cyberattack. [1]

1. Symantec
2. www.staysafeonline.org
3. National Cyber Security Alliance
4. CompTIA

IBT

DID YOU KNOW?

34% of businesses hit with malware take a week or more to regain access to their data!

The average cost of a ransomware attack on businesses is $133,000!

1. Sophos 2018 and Kaspersky 2018

IBT

CYBERSECURITY FRAMEWORK

NIST CYBERSECURITY FRAMEWORK

The framework is voluntary and provides your business an outline of best practices to help decide where to focus your time and money for protection.

1. IDENTIFY
2. PROTECT
3. DETECT
4. RESPOND
5. RECOVER

IBT

IDENTIFY

- Make a list of all equipment, software, and **data** you use
- Create and share a company cybersecurity policy that covers:
  - Role and responsibilities for employees, vendors, and anyone else with access to sensitive data.
  - Steps to take to protect against an attack and limit the damage if one occurs.

PROTECT

- Control who logs on to your network and uses computers
- Use security software to protect data
- Encrypt sensitive data, at rest and in transit
- Conduct regular backups of data and verify
- Update security software regularly
- Have formal policies for safely disposing of electronic files and old equipment
- Train everyone who uses your computers and network about cybersecurity. You can help employees understand their personal risk in addition to their crucial role in the workplace.

DETECT

- Monitor your computers for unauthorized personal access, devices (like USB drives), and software.
- Check your network for unauthorized users or connections.
- Investigate any unusual activities on your network or by your staff.

RESPOND

Have a plan for:

- Notifying customer, employees, and others whose data may be at risk.
- Keeping business operations up and running.
- Reporting the attack to law enforcement and other authorities.
- Investigating and containing an attack.
- Updating your cybersecurity policy and plan with lessons learned.
- Preparing for inadvertent events (like weather emergencies) that may put data at risk.

Test your plan regularly!

IBT

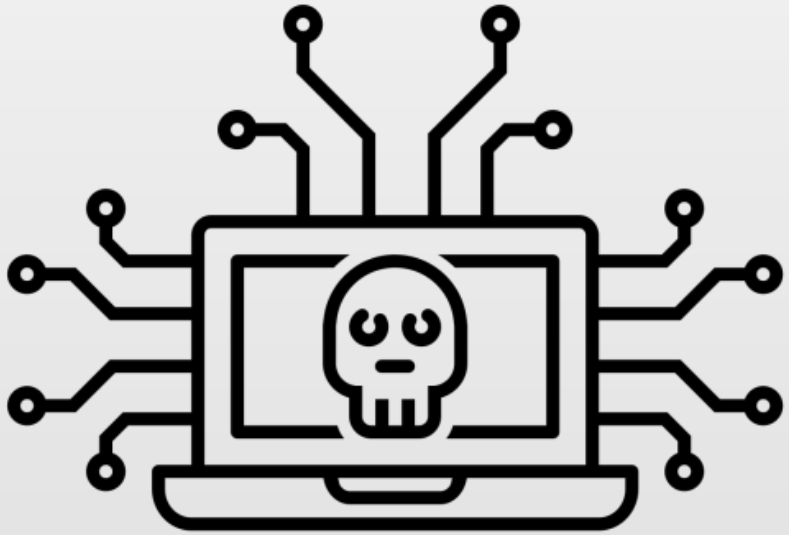
RECOVER

- After an attack:
  - Repair and restore the equipment and parts of your network that were affected.
  - Keep employees and customers informed of your response and recovery activities.

CYBER THREATS

Password Attacks: An attempt to decrypt or obtain a user's password with illegal intentions.

Ransomware: A type of malware that locks down and encrypts devices on a network to prevent someone from using a that device unless a ransom is paid.



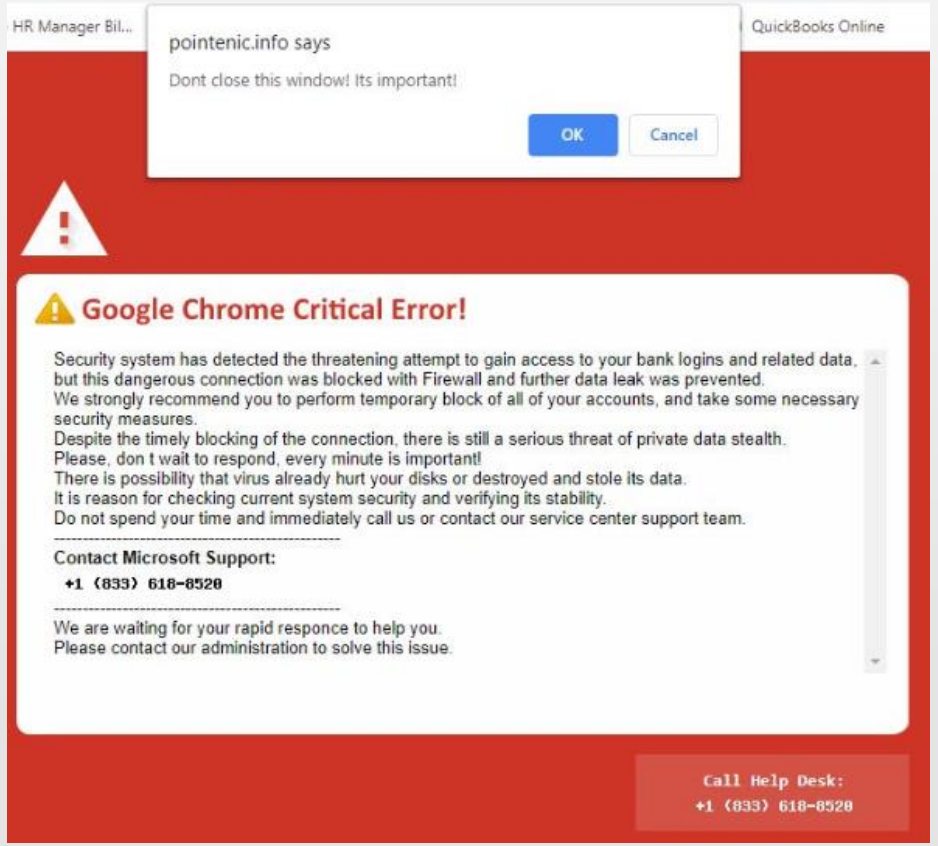
Phishing: A type of scam where criminals try to gain access to a network via email or other online social engineering methods to have you provide sensitive information, to gain network access.

IBT

CYBER THREATS

Scareware: malicious computer programs designed to trick a user into buying and downloading unnecessary and potentially dangerous software, such as fake antivirus protection.

Social Engineering: The use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.



Social Engineering Red Flags

FROM

- I don't recognize the sender's email address as someone **I ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address from a **suspicious domain** (like micorsoft-support.com)?
- **I don't know the sender personally** and they **were not vouched for** by someone I trust.
- **I don't have a business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I haven't communicated with recently.

TO

- I was cc'd on an email sent to one or more people, but **I don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a **big** red flag.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, www.bankofarnerica.com — the "m" is really two characters — "r" and "n."

DATE

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?

SUBJECT

- Did I get an email with a subject line that is **irrelevant** or **does not match** the message content?
- Is the email message a reply to something **I never sent or requested**?

ATTACHMENTS

- The sender included an email attachment that **I was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**. The only file type that is **always safe to click on is a .txt** file.

CONTENT

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar** or **spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd** or **illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?

KnowBe4
Human error. Conquered.

IBT

MISTAKE #1

ASSUMING IT WON'T HAPPEN TO YOU

From Wall Street to Main Street, large or small, companies in virtually every industry are vulnerable to attacks.

Don't assume that just because you aren't a huge enterprise, you aren't susceptible to cyber threats. Cybercriminals consistently target small businesses with stronger, more evolved threats.

IBT

SOLUTION

TAKE CYBERSECURITY SERIOUSLY.

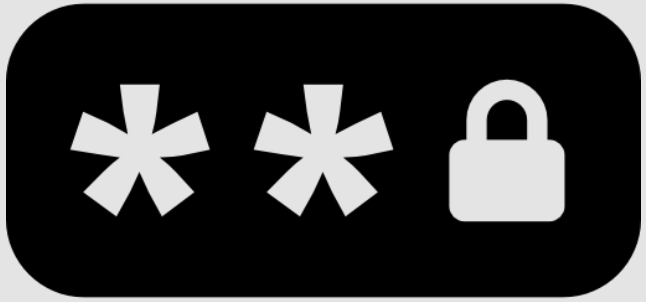
- **Change the mindset** and the culture of the organization. Assume you are a target.
- Make **cybersecurity planning** as important as other aspects of your business planning process.
- **Find qualified security experts** to help you conduct a risk assessment, identify cyber threats to your business, develop an incident response plan and implement countermeasures to mitigate high probability threats.

IBT

MISTAKE #2

WEAK AND VULNERABLE PASSWORDS

Weak passwords are continually cited by security experts as one of the leading factors making life easier for cyber-criminals. This is especially true as passwords, PINs (Personal Identification Numbers), and other number and letter-based codes are often the first line of defense for both private and business computer systems or mobile devices.



SOLUTION

CREATE AND USE STRONG, COMPLEX PASSWORDS.

DO NOT USE:

- Only letters or only numbers
- Names of spouses, children, grandchildren or dog
- Phone numbers, SSN or birth dates
- The same word as your log in or any variation of it
- Any word that can be found in the dictionary

Some of the worst passwords are

“Password,” “123456,” or your last name.

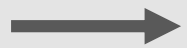
Source: https://www.consumer.ftc.gov/blog/advanced-password-tips-and-tricks

IBT

CREATING PASSWORDS

Tips to create passwords that are easy for you to remember but hard to hack:

- **Use a different password for each account.** If it gets stolen, your other accounts can't be taken over.
- **Get creative.** Mix letters, numbers, and special characters. Never use your name or birth date.
- **Use 12 characters if you can, but no less than 10.** The longer the password, the tougher it is to hack. Make it easier on yourself by using numbers and characters that resemble the letters they are replacing.



@ = a

1 = L

$ = S

0 = o

- **Change your password** several times per year.

Source: https://www.consumer.ftc.gov/blog/advanced-password-tips-and-tricks

IBT

MISTAKE #3

UNTRAINED EMPLOYEES

People are the weakest link in any organization's cybersecurity defenses.

In this era of the social media platform, too many of us reveal intimate or specific details on our personal and working lives – the kind of information which, combined with data from user profiles, company websites, and numerous other sources, can give cyber-criminals access to complete digital identities, transaction records, or financial profiles.

IBT

HUMAN FIREWALL

People are the last line of defense!

91% of successful data breaches start with a spear phishing attack

30% of data breaches are caused by repeat offenders from within the organization

IBT

TOP CLICKED PHISHING TESTS

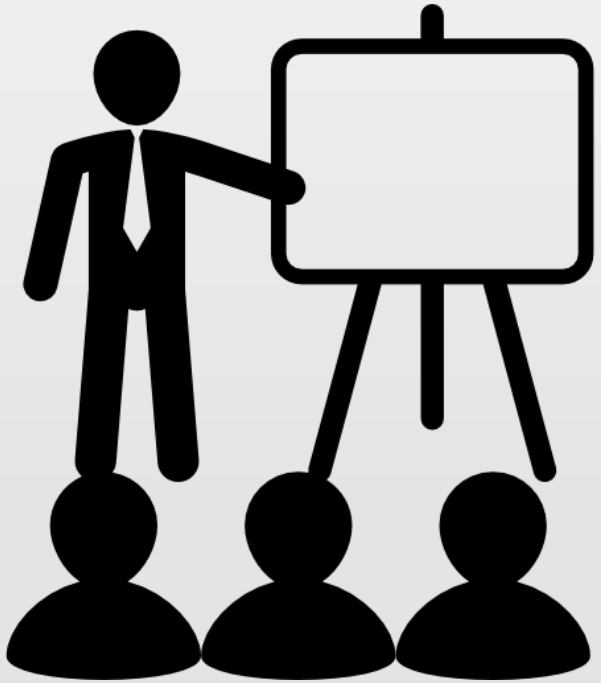
1. LinkedIn – Join My Network, Profile Views, Add Me, Deactivation Request – 56%
2. Login alert for Chrome – 9%
3. 55th Anniversary and Free Pizza – 8%
4. Your Friend Tagged a Photo of You – 8%
5. Facebook Password Reset Verification – 8%
6. Your password was successfully reset – 6%
7. New Voice Message At 1:23AM – 5%

IBT

SOLUTION

SECURITY AWARENESS TRAINING

While it may seem unnecessary to train every employee on how to avoid cyber threats, it could save your company enormous loss. You should regularly re-train both remote and in-house employees to use secure protocols, think before they click, guard against stolen devices and take action the second an attack takes place.



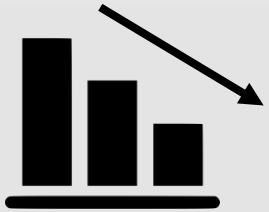
SECURITY AWARENESS TRAINING

KnowBe4
Human error. Conquered.

The world's most popular integrated platform for awareness training

TRAIN YOUR USERS

PHISH YOUR USERS



SEE THE RESULTS

IBT

SOCIAL MEDIA SECURITY

Tips For Playing It Safe on Social Media:

Selectively share information.

Set profiles to private.

Make passwords strong and unique.

Lock your device.

Think before you post.

Source:
http://www.huffingtonpost.com/entry/identity-theft-through-social-media-8-ways-to-protect_us_58ab27c9e4b0fa149f9ac937

IBT

MISTAKE #4

RELYING SOLELY ON ANTI-VIRUS TECHNOLOGIES

In today's sophisticated threat landscape, anti-virus technologies alone are not sufficient to prevent persistent and advanced attacks.

75% of companies infected with ransomware are running up-to-date endpoint protection

IBT

SOLUTION

CONSULT WITH EXPERTS

Anti-virus software is still useful and must be kept up-to-date. However, to thoroughly secure your data, it's a good idea to use IT service providers who have the specialized knowledge, resources and abilities to help you come up with a thorough security policy and employee awareness plan.

MISTAKE #5

FAILURE TO BACK UP

This is something that most businesses tend to overlook time and again. The fact is, backing up your system can actually come in handy at times when cybersecurity is breached.

SOLUTION

BACKUP DISASTER RECOVERY

With a Backup & Disaster Recovery (BDR) Device, you can have peace of mind knowing your data is always safe. It is a quick, secure and temporary solution that gets you back to work with minimal downtime.

IBT

ADVANCED SOLUTIONS

Autonomous Endpoint Security

Artificial Intelligence (AI) Driven Intrusion Protection

Enhanced SPAM Filtering

Two Factor Authentication

Advanced File System Security

Next-Generation Firewalls with UTM and IDS

Managed Detection and Response (MDR)

Email Encryption

Virtual Private Network (VPN)

IBT

If you have any other questions about cyber threats or want to protect your business, please let us know. We will bring you the best solutions and help your company stay proactive before an attack happens.

IBT

THANK YOU!

Eric Kehmeier
ekehmeier@IBTsupport.com
www.IBTsupport.com
918.770.8738

Integrated Business Technologies
1800 South Elm Pl., Suite 200 / Broken Arrow, OK
918.770.8738 / www.IBTsupport.com