BluLin

Blulin.com

Data Security 101

The Essential Guide for Businesses

BluLin

Data Security 101: The Essential Guide for Businesses

In the current industry climate, data security is rightly one of the biggest concerns for modern businesses.

What the examples on this page should tell you is that no company is safe—if these giants couldn't keep their data safe, how can small and mid-sized businesses? A good place to start is understanding where your company's IT systems currently stand and the basics of keeping them safe.

Notable Recent Breaches

Gmail hack, March 2017

A harmless-looking Google Doc link went out to thousands of Gmail accounts. Because it looked legitimate many saw the email as a typical doc share and thought nothing of clicking.

Ransomware attack, June 2017

Malware spread across the computers of thousands of users, ultimately infecting several international corporations.

HBO hack, July 2017

Hackers stole 1.5 terabytes of private data from HBO's servers, including much anticipated series releases and sensitive employee information.

Could you be doing better?

Boundaries to Good Security

Companies face a slew of challenges when it comes to keeping their data secure.

Lack of Awareness

Some businesses are not aware of the risks involved until they actually run up against a problem.

Lack of Education

Even if they know about data security issues, they may now know how to go about tackling them.

Lack of Resources

Some businesses don't have the resources for an in-house person dedicated to data security, and assume they are stuck with their current setup.

Lack of Time

Most businesses are focused on doing what makes them money instead of worrying about potential tech problems. This is particularly true of small and mid-sized business that are growing quickly and trying to make their systems keep up.

Let's cover data best practices.

Data security is an ongoing challenge for everyone, but the best practices in this guide, when implemented, should give companies a reasonable shot at avoiding the biggest data security problems.

Unit 1

Basic Security Systems

Antivirus

Every computer in your office should have a basic level of antivirus software to protect against baseline-level threats—the kinds of risks every business encounters in its day-to-day operations.

This includes document sharing, Internet use, and other business activities.

KEY AUDIT QUESTIONS:

- What antivirus do your systems use?
- How well-rated is your antivirus software, as compared with others?
- Has it been updated lately? Does it automatically update with the latest virus definitions?
- Is your antivirus software adequate for the industry you're in?

Firewalls

Every company should have a basic firewall set up to screen out the most common hackers, viruses, and other malware that tries to reach your systems via the Internet.

Most common operating systems, like Windows and Apple OSX, have built in firewalls, but that's often not enough for businesses who work with sensitive client information every day. A more robust firewall that's customized for your needs is a good option for most businesses.

KEY AUDIT QUESTIONS:

- Do your computers and other systems have a firewall turned on?
- Are you aware of its parameters and how they affect your level of protection?
- Are there remaining risks you need to consider beyond your current firewall?
- Are you aware of the aspects of your network that are not protected by the firewall?

Unit 1

Basic Security Systems

Password Security & Management

Your personnel will likely have their own passwords to log in to their company accounts and computers. However, occasionally, businesses may have multiple employees using the same credentials to access a website or piece of software.

Either way, password management is crucially important for data security.

KEY AUDIT QUESTIONS:

- Do your employees' passwords follow industry best practices, and are they stored anywhere on your system?
- If you have common passwords, are you following best practices for storing these?
- Have you considered implementing a password manager?
- Do you have adequate security for password reset features to prevent them from being used by wrong parties?

Encryption for Mobile Devices

The nature of work in the modern office has grown to include the use of mobile devices such as laptops, tablets, and mobile phones. When these devices go off-site, it becomes much harder to control them.

Adding a level of encryption can ensure that these devices can't be unlocked should they fall into the wrong hands. Each type of mobile device has its own encryption best practices that should be followed.

KEY AUDIT QUESTIONS:

- If your employees utilize mobile devices for work, are these encrypted?
- Is data from encrypted mobile devices periodically backed up in case of loss of the device?
- Do your mobile devices include malware protection to prevent data leaks?
- Are you aware of the benefits of implementing a mobile device management (MDM) platform?

Unit 2

Four Tips to Better Backups

No matter how secure, no business is safe from things like hardware malfunction, user error, or natural disasters. That's why backups are one of the best things you can do for your data security. Simply creating this redundancy enables you to know you always have an extra copy of your data stored safely away.

1. Decide on a storage option.

Based on the amount of data you'll be backing up, you may choose to store the data locally, on remote servers, or in the cloud.

2. Decide on a frequency.

This is again determined by how much data you're storing and how quickly that data changes. You'll want to back up at least once a month, but some businesses find it worthwhile to run backups weekly, or even daily.

3. Deal with capacity issues.

Backups are important, but depending on your business, they can take up a lot of space. Inevitably, old backups need to be deleted to make room for new ones.

You'll need to decide how far back you want to keep data. Is last month's backup good enough, or do you need backups going back 3 months?

4. Automate the backups.

One of the key issues with backups is compliance—when there are other things to do, it's hard to think about backing up your data. Setting up an automated backup process will make sure it gets done without having to think about it.

Unit 3

Training Your Team

One recent study found that employees, rather than IT systems, are the highest “risk” of data breach. What that means is that no matter how secure your systems are, an employee can always make a mistake and compromise your systems.

Email

From phishing schemes to identifying potentially compromised files that could be ransomware, employees need to know how to spot potentially harmful emails.

Password Management

In their day to day, your employees likely use a variety of tools with different passwords, and they need to know the best practices for creating passwords that are tough to crack.

Physical Security

Mobile devices such as laptops and cell phones should always be monitored and never left in vehicles or public places. Computers at workstations should be locked anytime the employee leaves his or her desk.

Software Installation

Day-to-day, employees might be tempted to install the latest version of Java, Adobe, or another piece of basic software. Establish rules about which updates can be done by employees and which require an IT person.

Appropriate Internet Use

Employees need clear guidelines on what types of websites are appropriate and inappropriate at work, and which ones

Learn to spot a dangerous email with our easy infographic on the next page!

How to Recognizing Suspicious Emails: Questions to Ask

Subject

Does the subject line makes sense and fit the rest of the message?

Is it relevant to your role at your organization?

Is the subject line a RE: to a message you never originally sent?

From

Do you recognize the sender's email address? Is it a known contact?

If you don't recognize the email address, does the domain look suspicious?

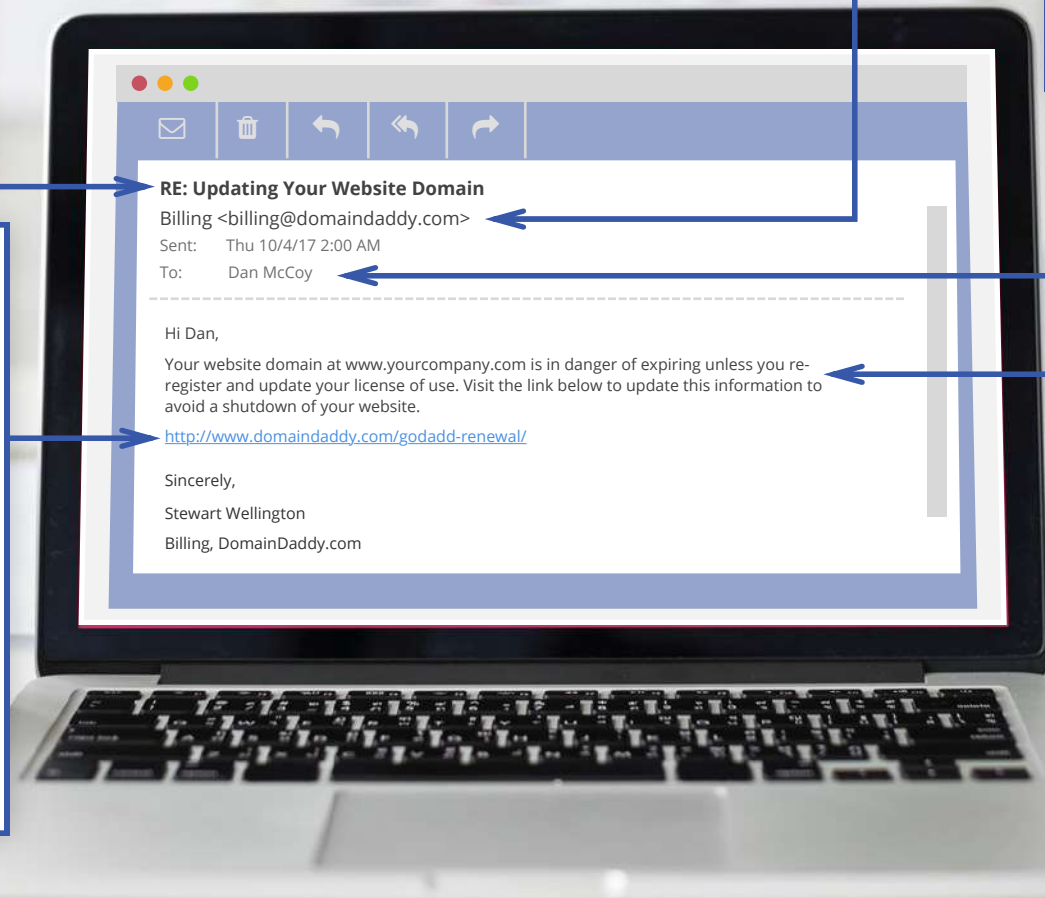
Is this email from someone outside your organization that you've never done business with?

Is the email from someone inside your organization, but unusual for that person?

To

Is this an email you were cc'd on that's going out to a list of people you don't know?

If you do know the other recipients, are they an unusual mix, such as across management levels or with names only starting with one letter?



Links & Attachements

Does the email include an attachment of unusual nature or that you were not expecting?

Does the email include unusually long hyperlinks?

When hovering over the hyperlink, does a different URL show up than the one the link indicates?

Does the link attempt to imitate a well known website or company (such as http//:appple.com)?

Content

Does the email as you to click on a link or view an attachment in order to avoid something bad (e.g. your inbox is out of space), or gain something unusual?

Does the email have grammar, spelling, or formatting problems that seem unusual coming from its supposed sender?

BluLin

Find the right IT solution for your growing business.

"If you seek a trustworthy, hardworking and intelligent IT support staff, BluLin IT is the way to go. The owner Matt and his team will never tell you 'no,' they will just get things done. They always act with your best interest in mind. I put choosing them among the 10 best business decisions I have ever made."

- Jim Rozell, Founder & CEO of Hotel Compete

What we do at BluLin.

IT Consulting & Strategy Planning

Client Portal for Employees

On-Site Support & Emergency Response

Server & PC Management

Server Backup Solutions

Help Desk

Get in touch with us!

(312) 267-1111

555 W Jackson Blvd Ste 700
Chicago, IL 60661

Learn more about us at blulin.com!