

7 Cybersecurity Tips To Build A Secure Website That Creates A Trusting Consumer Relationship

LME Services' VP of Business Development Joe Engelking shares how to ensure sensitive data is protected, why cybersecurity improves brand credibility & more.

NEW YORK, NY, UNITED STATES, December 19, 2018 / EINPresswire.com/ -- [According to Norton](#), the U.S. will account for half of all data breaches by the year 2023.

So although cybersecurity might seem out of sight, out of mind, online criminal activity actually poses a real threat to your sensitive data, internal information, and consumer base.

Luckily, there are measures you can take to protect yourself from malware and data breaches.

We sat down with Joe Engelking, Vice President of Business Development at [LME Services](#) -- a leading web development and cybersecurity company -- to learn how to invest in valuable cybersecurity, why security measures benefit your business, how to design a professional web design that's credible to consumers and more.

DesignRush: Cybersecurity is a key offering of LME Services. How does investing in cybersecurity ultimately improve a business's success? What are the top benefits?

Joe Engelking: Cybersecurity covers a lot of things but its main advantage is to reduce downtime, stop productivity drains and minimize the likelihood of legal issues.

Another major, and often ignored, aspect of cybersecurity investment is it that it helps



businesses to avoid crippling legal issues.

E.G., if you house sensitive client data (HIPAA covered items, for example) there are severe financial repercussions for not properly protecting your client's personal information (especially for those housing EU information under the new GDPR rules).

For those not worried about sensitive info being stolen, then reducing the likelihood of downtime and productivity are the main advantage.

'Hackers' these days want to encrypt/steal your data and to them, it's simply a numbers game because they know that every business has a couple of, shall we say, easy targets.

So, let's just imagine that a hacker gets your password (whether through phishing emails or repeatedly attempting your passwords through brute force) and they then deposit a ransomware virus on your servers which encrypts and locks all your files.

When an attack like this is successful (and these viruses are successful surprisingly often) ask yourself how much time and production you would lose.

If your main file repository or mail system went down and could not be restored, or takes days to get back up and running.

These online criminals want to cripple your data/communication so that they can either extort you for a lot of money and/or mine your data for banking info for a bigger score.

Norton estimates that Hacker's stole nearly \$20 billion from American's last year with those numbers expected climb.

Cybersecurity means protecting yourself from these common and foreseeable scenarios by implementing simple measures to severely diminish the likelihood of becoming their victim.

DR: Businesses are relying on digital platforms more and more. What are 3 tips that they can employ to ensure their sensitive data and information is protected well?

JM: For overall cybersecurity protection, we ask businesses to invest in three things:

1. Get Spam Filtering setup to catch all those damn phishing emails – phishers are typically way cleverer than your average employee. They send millions of emails and have finely tuned their spam to look like its coming from reliable brands (and no, having a JUNK folder in outlook does not count as spam filtering).

2. Have a backup of all your key systems and data (with a 'backup server' if you can afford it, which will be sitting there ready to spin-up any downed servers or systems). When businesses back up everything or have a backup server in place, their employees can still work as normal should something happen on your network. It is unfathomable to me that so many businesses have NO BACKUP (it's insanity really), or worse yet they 'think they have tape backup' and when I go to check it, it hasn't successfully recorded a backup since Bush was president.

3. Enable some kind of virus or malware protection with alerting. Trust me, employees do not want to admit they fell for a scam. They will often not tell IT or admin staff they are infected until it severely hampers their computer or your server. Malware alerts can make it easy for businesses to scan anything that might be harmful to their digital infrastructure before it becomes a large-scale issue.

A fourth protection item we recommend is MFA -- or multi-factor authentication -- which you've probably set that up on your banking sites.

MFA is when you enter a password and then have a second authentication procedure, like answering a phone call or text.

This extra level of security is absolutely vital to limiting the likelihood of becoming a victim because not only does a hacker need your password but they would also need access to your cell phone.

We also recommend that you teach your staff proper internet browsing and how to recognize fake emails.

DR: How can businesses build professional websites with cybersecurity in mind?

JM: You will want to make sure you have Captcha on any and all logins or forms because as soon as a bot gets access to a blog forum or newsletter sign-up, you are going to get more information about male-enhancement than you could possibly need.

Also, have a backup of your website should it get attacked, you can pay \$100 for a site backup or \$5000 to have the site rebuilt, do the math.

Don't add any plugins, CSS code or add-ins to your website that you aren't 100% sure are safe and legit and it's probably worth investing in your own hosting server.

Many businesses purchase shared hosting when they go through GoDaddy or Network Solutions, which means that for a reduced cost, instead of having your own secluded web server you are in fact sharing a web server with a bunch of other random websites.

The risk of these shared hosting plans is if another website on your shared web server gets hacked or compromised, there is a change that virus will spread to your website even though you do nothing anything wrong.

Paying a little extra money for an individual hosting plan is, therefore, a great way to reduce risk to your website.

Having an SSL certificate is also a great way to secure people's activity on your site.

Once you have the SSL certificate, make sure you default your website to be on HTTPS rather than HTTP - and if you are unsure how to do this you can always reach out to us for assistance.

HTTPS basically ensures that activity and communication done on your website is encrypted and secure.

Also, add MFA to anyone who accesses your website, so that even if a password does get lost, people won't be able to get in and wreck anything.

DR: Speaking of website design, LME Services offers web development too. What advice do you have for businesses who are hoping to improve their online presence and capture consumers?

JM: First off, we believe that people need to focus on their online presence first, and then have their website fit into that rather than the other way around.

Everything that people can find about you online needs to be cohesive and create a positive and inviting picture of your offerings.

Simply Google your business and make sure that everything on the first page all says and re-emphasizes the same core message.

Your online presence starts with SEO, or search engine optimization, and this is where businesses make or break their online success (I actually have a blog post about how I got 200 daily visitors and am now nearing 300).

A sharp looking, thoughtfully designed website is the first step.

Make sure it's clear what you do, what you are offering and why you are the right choice by having examples of social proof (badges, awards, reviews, etc.).

Keep text short and to the point, because NO ONE reads longwinded pages (also make sure your site is mobile-friendly).

Have calls to action (contact forms, signups, webinars, newsletters, consultations, etc.) and landing pages. Never run an online ad that sends people to your home page, when you run an ad or are driving traffic to your site for a specific thing, then have a page dedicated to that traffic that speaks exactly to why they came to your site and why you are the right choice.

Nothing is worse than seeing people pay for online ads only to have those ads drive people to your homepage, such a wasted opportunity.

From the SEO perspective, either hire an SEO person or do it yourself. For search engine optimization to be successful, you need to make sure that you are on page 1 for any and all lucrative search terms for your industry.

If you're a dentist in Chicago, make sure your website has that clearly posted in your headlines, page titles and Meta descriptions.

Don't have a website with crappy stock photos and pointless jargon that confuses people, nothing is worse than succumbing your hard won web traffic to awful introductions like "You can count on _____", or "welcome to our website!".

Ugh!

Also, make sure to completely fill out your Google and Bing Business profiles.

You should also try and get other important websites to link to your website. Those links are massively important. On top of your Google and Bing business pages, submit your business into online directories like Yelp, Angie's List, YP and any industry-specific sites.

Once the website and SEO are tight, monitor your traffic with tools like Google Analytics and Clicky and then see what's working and what isn't. This will help inform your digital strategies going forward.

DR: Tell us about some projects your agency has worked on. What elements made it a success and what did you learn?

JM: We've done a fair amount of Office 365 migrations. These include the migration of email, calendars, and contacts, as well as the migration of servers and business system to the cloud (Azure, AWS, SharePoint, Google Drive).

The success was, in large part, because we made sure to speak with the engineers of the platforms beforehand to ensure a smooth transition. We also communicated with our clients to create a clear schedule and made sure to emphasize to our clients that these migrations are very involved and require a lot of skill to pull off.

By making them aware of the challenges and by being prepared and scheduling everything we were able to make the cut over to the cloud on the weekend and with little downtime and that there weren't unreal expectations on the client's side. Communication is key.

We've also worked on a firewall and wireless implementation project which involved mesh wireless networking for simplified wireless usage, a Cisco firewall setup and administration of their Anti-Virus, spam filtering, backups.

We also offered some of their staff a productivity assistance session where we sit with people and review their work process and offer ways to increase their productivity by removing steps, teaching them new tools and hotkeys, designing shortcuts, etc.).

These sessions help to increase productivity anywhere from 2-15%.

When taking over a client we try to explain why we want to implement certain systems and procedures and then walk them through why it will be better for them. We learned that people just want things to work but typically respond better to new ideas or systems when you can clearly explain why a "firewall" or "mesh network" will simplify their life. Explain the benefits with simple analogies so that what you are doing makes sense to them and avoid using buzzwords and fancy acronyms, it just annoys people.

Finally, we do a lot of web design and SEO work – most notably was for a law firm in California where we handled all of their web design and search engine optimization services.

The success of this project was due in large part to the analytics. After we did our initial on-page and off-page work we were able to clearly showcase the traffic increase we created and how, through better page design, were able to increase traffic conversion.

We learned that SEO is not all that complicated once you understand how search engines work, what visitors are looking and what Google wants from your page. With those 3 things covered, you can greatly increase the visibility and conversion percentages of your online presence.

DR: Every business ultimately hopes to generate leads and increase revenue. Which digital services or web design strategies will help brands achieve this quickly and provide a great return on investment?

JM: Your business needs a modern website that clearly speaks to your target audience, and that site needs proper SEO applied to it and which actively attempts to either grab the visitors or gets the visitor to reach out to you.

For less than \$5,000, you can very easily build a website that will be at the top of search engines for your services.

By virtue of the fact that most businesses ignore Google and what it wants from your website, you can very easily just do a good job on design and SEO and immediately make your business look more professional, modern and capable than the throngs of dullards who either ignore their online presence or who think simply having a generic website is enough.

We creative, be different, stand out! Make a list of why your competitor's websites suck and then do a better job!

Whether we like it or not, we make immediate decisions about a company based on their website. If you see an old, out of date website, then you are going to think that company is out of date and incompetent, conversely, if you see a modern and aesthetically pleasing site, you are going to assume that business is more modern and better to work with.

Compare [top web design agencies](#) who can create a safe and secure website by expertise, price, reviews and more in DesignRush's agency listing section.

Stephanie M Sharlow

DesignRush

+1 4193566394

[email us here](#)

Visit us on social media:

[Facebook](#)

[Twitter](#)

[LinkedIn](#)

This press release can be viewed online at: <http://www.einpresswire.com>

Disclaimer: If you have any questions regarding information in this press release please contact the company listed in the press release. Please do not contact EIN Presswire. We will be unable to assist you with your inquiry. EIN Presswire disclaims any content contained in these releases. © 1995-2018 IPD Group, Inc. All Right Reserved.