THE WITTMANN AGENCY

Love Letters To Bookworms | Liebesbriefe an Bücherwürmer

Global Online Marketing + Strategy For Modern Publishing Entrepreneurs

Reading time 4 min 41 sec

Servus*, my dear First Name !

It’s a tale of modern digital times – running our businesses without any security issues.

You may have noticed: COVID-19 sparks an upward trend in cybercrime.

Fact is, that EVERY business, large or small, is a possible target for hackers and cybercriminals.

Small and medium-sized businesses are most vulnerable to cyberattacks and newer forms of malware because there is less sophistication in the cybersecurity along with greater ease for hackers to take information or financial resources.

I’ve had clients, colleagues and friends, who had their sites removed, E-Mail hacked, passwords changed and data were stolen.

You may think now, OMG, what happens when...

- you get hacked?
- you’ve given an all-access pass to your online identities (website, Facebook page, Twitter feed) to an intern, assistant, employee or friend and the relationship goes sour?
- your business partner goes out of business or just disappears?

Don’t worry, First Name, you're not alone!

I’ve had more than my fair share of pain: A lightning strike destroyed all my electronic devices at once, I had to set up a new website to take back control of my own business site and my amazon merchant account got hacked during the pandemic just to name a few. After (a lot of) trial and error, here's my list of

Cyber-security mistakes you should avoid in 2020 and beyond

BACKUP

#1 Backup your website and data regularly
Yas, we always say we’ll do this...kind of like writing our last will and flossing our teeth...

Ninja Tip: Follow the 3-2-1- Backup Rule, which means, keep at least three (3) copies of your

data, and store two (2) backup copies on different storage media, with one (1) of them located offsite.

At least try to do this once a month (website), once a week (data) — put it on the calendar!

What I use and trust for my business:
(I only recommend services and tools that I actually use in my own business):

Cloud storage: Alfadrive by Alfahosting and Dropbox*
External hard drive: LaCie MOBILE DRIVE and Intenso

PASSWORD

#1 Store your passwords in an easily accessible and secure location.
I personally use password-protected spreadsheets stored on my computer system, my cloud and hard drive, but there are numerous online password systems, too.

Ninja Tip: Please don't use yellow notes taped to the computer system you're using and think twice before sharing your passwords with others – you're just inviting people to hack into your accounts.

#2 Change your passwords
When someone who has access to your accounts (intern, employee, business partner etc) is removed from your network or company, make sure you change the passwords for all accounts.

Ninja Tip: Think of yourself as a digital landlord changing the locks after a tenant moves out and a new one is about to move in.

Make sure to change passwords and remove extra accounts for your:

- Website
- Web host (Alfahosting, WP Engine etc)
- Cloud Storage (Alfadrive, Dropbox*, Google Drive etc)
- E-Mail account(s)
- E-Mail newsletter service (Cleverreach*, Mailerlite etc)
- FTP account
- Twitter, Facebook and any other social media accounts (YouTube, Vimeo, Spotify etc)
- Online scheduler (Calendly, Acuity, Zapier etc)
- Paypal, merchant accounts and any other online service accounts

What I do in my business:
I set up separate accounts just for them – then you can easily delete their accounts.

#3 Use strong passwords
It's easy to use your pet's name, your birthday or the most used (poor) "12345" but use strong passwords whenever possible.

A strong password
#1 has at least **15 characters**
#2 has **uppercase letters**
#3 has **lowercase letters**
#4 has **numbers**
#5 is **not** like your **previous passwords**
#6 is **not** your **name**
#7 is **not** your **login**
#8 is **not** your **friend's name**
#9 is **not** your **family member's name**
#10 is **not** a dictionary **word**
#11 is **not** a **common name**
#12 is **not** a **keyboard pattern**, such as qwerty, asdfghjkl, or 12345678
#13 has **symbols**, such as ` ! " ? $? % ^ & * ( ) _ - + = { [}] : ; @ ' ~ # | \ < , > . ? /

Google "strong password generator" to find free online services that instantly generate complex passwords that combine letters, numbers and special characters.

Ninja Tip: "password" isn't a strong password either.

#4 Let them know and make sure you're watching
Make it a part of your business that any malicious online activity will be monitored and not tolerated.

There are great plugins to monitor activity on WordPress (website, blog, landing page). If you use Google's Gmail, you can track what IP addresses accessed your account.

Stay safe, First Name, I'm sending you enormous love & strength.

All my ❤️,
xoxo Claudia

P.S. *Bavarian's infamous *Servus*, means "Hello, how are you?" in Germany and Austria.

P.S.S. If you love a post, please leave a comment (I read and love every one of them) and share! Share it on Facebook, share it on Twitter, share it wherever you share. I know who my best sharers are, and love them longtime.

P.S.S.S. If you think my digital workbook 5 Mistakes Even Smart Publishing Professionals Make and the fixes, is most helpful, you can't afford to miss my digital guide 25 Digital Marketing Tools And Services Modern Publishing Entrepreneurs Can Trust, which is the perfect complement to this workbook.

P.S.S.S.S. *Affiliate Disclaimer: I am a firm believer in complete transparency. From time to time I may make recommendations for products and services that I truly believe in. A freelancer since 2011, I have used and relied on many online products, both free and paid, and it is my goal to help you be successful online. By providing links to certain products and service providers, I may earn an affiliate commission (market with a pink asterisk*) for any purchases you make. I only promote those businesses and services that I have really used myself and trust for my day to day business. Please note that I have not been given any free products, services or anything else by these companies in exchange for discussing them on my site. If you have any questions regarding

the above, please do not hesitate to contact me.

Want even MORE?

- Weekly motivation
- Curated tips & tools & deals
- Exclusive giveaways

Well, today's the day. This year's your year.

LOVE LETTERS TO BOOKWORMS | MAGAZINES FOR BOOK LOVERS

For occasional (and awesome) social updates, here is where to find us.
YouTube - Twitter - Pinterest - Xing - Kress

Pssst! If you forget why you're hearing from me, Claudia Wittmann, it's probably because you signed up for a superb freebie on my site, www.the-wittmann-agency.com. If you don't want these E-Mails, you can say "Bye, bye" any time. | Note that any links might be affiliate links. I sell things sometimes.

Wenn Sie diese E-Mail nicht mehr empfangen möchten, können Sie diese **hier** abbestellen.

Our Legal Notice & Data Privacy Statement

You are subscribed to The Wittmann Agency's global e-Newsletter. If you wish to unsubscribe **click here.**

The Wittmann Agency
Lutherstrasse 23
06886 Lutherstadt Wittenberg
Deutschland | Germany
contact@the-wittmann-agency.com
www.the-wittmann-agency.com
USt.-IdNr. / VAT-Nr. DE279052110