frogworks

Managing Your Technology So Your Business Doesn't Croak.

February 2023

Issue 1 Volume 13

Ribb"IT" Review

INSIDE THIS ISSUE:

- Internet Security
- What Makes a Good Password?
- Risks of Public Wi-Fi

Internet Security Tips

In this digital age, you and your company's website is a crucial part of your business. You want it to look professional, as well as be easily navigable and highly engaging. But you don't just want a website that looks nice and has an intuitive user interface (UI) — you also want a website that's *secure*.

Website security, despite being a vital part of your overall cybersecurity posture, is far too often overlooked by small and medium-sized business (SMB) owners. As with many aspects of cybersecurity, there is an enduring belief that hackers don't come after 'the little guy.' And so, business owners put 'improve website security' at the bottom of their to-do lists, thinking it can wait.

But the truth is, the 'we're too small' justification for neglecting website security is paper thin; we're seeing threat actors target smaller companies more and A recent study revealed that 61% of business's have experienced a cyberattack over the past year. Cyberattacks on SMBs aren't rare, they're rampant, and beefing up your website's security isn't preparing for a possibility, but bracing for an inevitability.

This monthly publication provided courtesy of:
Alex Bleam,
Owner of Frogworks

Continue reading for four internet security tips!

Internet Security Tips:

1 Practice Good Password Hygiene

Your passwords are a critical line of defense against cyberattacks. Unfortunately, poor ‘password hygiene’ is practically an epidemic, even in this dangerous digital era. Get serious about practicing good password hygiene at your business or at home. Set up password complexity requirements on your company’s website, train yourself /staff on what makes a strong password.

2 Keep Up with Updates

Like any piece of property, your patch of digital land requires maintenance. You have to keep up with software and plugin update requests. you’ve ignored cell phone updates before and it’s not like your whole life came crashing down …Stop right there! Updates are not optional enhancements; they’re necessary adaptations to an ever-evolving threat landscape. And if you’re casual about updates, you’re putting your entire organization at risk.

3 Backup, Backup, and More Backup!

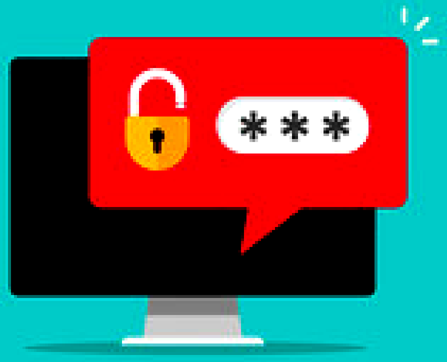
Similar to updates, data backup is a security fundamental you can’t afford to neglect. No matter how careful you are, things happen , cyberattacks, natural disasters, simple employee errors, and data gets lost. But when the data you lose is backed up i.e., when there’s a copy of it it’s not truly lost. You swap in the copy and you’re back on your feet.

4 Train Your Staff

The importance of employee training cannot be overstated. Your people are your most valuable asset this isn’t just true as a general adage, but as a principle of cybersecurity! If there is one thing any business can do to immediately bolster its website security, it’s implement regular staff training. Whatever training regimen you come up with, stick with it. Cyber risk training should be ongoing and regular.

(Protecting your growing business means protecting its website. And while following the above tips won’t guarantee your website’s total security ,sadly, no such guarantees exist , they will go a long way toward protecting your organizational and customer data, and keeping hackers off your digital land.)

What makes a Good Password?



As more and more of our lives move online, we end up accumulating more and more accounts each of which has its own password. It feels like almost every site has its own policy, ranging from lax to inane. But, is _4$% nT;6**a_ really safer than _Butterfly5Cat5WaffleIron_? What really makes a good password? A password’s strength is governed by its bits of entropy. Password entropy is a measurement of how unpredictable a password is.

(To generate a secure password, you need to increase the complexity and length)

Reusing Passwords:

We all have a million accounts and it gets frustrating accounting for every password. For this reason, many people reuse identical passwords. Reuse of a password compromises it in a way which bits of entropy can’t account for. When a site is compromised an attacker can easily take your password that has been reused on other sites and gain access to those other sites.

The traditional view of password security was that the more complex the better, though this is just one small part of the picture. The length plays in as much as the complexity. An extremely complex password which is short is as bad as an extremely simple password which is longer. A longer password with a mix of upper and lowercase letters, symbols, and numbers help make your passwords more secure.

Word Search

K	S	X	O	A	R	I	C	J	N	H	H	T	I	P
Y	E	D	Y	M	W	T	O	E	P	D	V	O	K	L
P	R	U	V	Z	N	R	M	P	B	C	U	T	S	T
C	V	O	S	U	L	F	P	A	C	C	E	S	S	G
K	E	L	O	S	M	O	U	H	T	Y	E	R	F	T
G	R	C	J	N	J	T	T	O	I	C	E	Q	P	M
R	C	H	Y	B	V	G	E	J	U	S	Q	Q	A	D
A	O	P	P	N	D	J	R	R	L	K	H	P	J	O
N	X	A	N	M	D	X	I	Y	X	Y	S	I	A	W
W	O	S	H	N	E	T	W	O	R	K	V	O	N	N
G	Z	S	K	V	Y	H	H	Y	H	G	R	O	Y	G
Y	H	W	P	I	P	U	K	C	A	B	M	X	P	L
F	S	O	F	F	J	E	Q	W	E	B	S	I	T	E
X	A	R	G	I	X	L	U	B	W	Q	G	R	K	L
C	R	D	T	W	S	X	M	E	C	Y	B	E	R	T

COMPUTER
BACKUP
ACCOUNT
CYBER
SPAM
WIFI
CLOUD
WEBSITE
NETWORK
PHISHING
SERVER
ACCESS
PASSWORD
SECURITY

Always exercise caution when downloading files or conducting other online transactions. For example, never download anything from an unknown website or email. It may be a phishing attempt to steal personal or financial information. When traveling for business or pleasure, it's important to know that there are a number of security risks associated with public Wi-Fi. However, by following a few simple guidelines, you can protect your data and stay safe while browsing the internet.

Risks of Public Wi-fi

Public wi-fi offers a convenient way to stay connected while out or traveling. If a hacker intercepts your data while using public Wi-Fi, it can result in identity theft, compromised credentials, malware exposure, or even compromise your business account. The best way to ensure that information is protected online is to use HTTPS when available. HTTPS is a secure protocol that encrypts all data sent between a website and its visitors so that no one can intercept and steal the information. However, not all websites offer HTTPS. Users can utilize a VPN to protect their data further. A VPN will encrypt users' data as they navigate the internet, protecting their valuable information.

We Have an E-Newsletter!!!

Do we have your e-mail address??? If you would like to receive our newsletter though email please visit us at:

www.getfrogworks.com/newsletter

Channel Futures
Leading Channel Partners Forward
NEXTGEN 101
MSP TO WATCH • 2021 WINNER