TECHNOLOGY TIMES

"Insider Tips To Make Your Business Run Faster, Easier And More Profitably"

Don't Make This Critical Mistake In Your Business

Upward of 41% of companies don't train their HR staff on data security. This is from a recent survey from GetApp. On top of this, 55% of HR staff don't see internal data security as an issue.

Read More Here:

www.optistartech.com/HR

March 2020

This monthly publication provided courtesy of Mark Jordan, President of Optistar Technology Consultants

Our Mission :

To help small businesses succeed by providing the highest quality IT CONSULTING, solutions and support money can buy.

5 Signs You're About To Get Hacked — And What You Can Do To Prevent It

Hackers love to go after small businesses. There are many businesses to choose from, and many don't invest in good IT security. Plus, many business owners and their employees have bad cyber security habits. They do things that increase their risk of a malware attack or a cyber-attack. Here are five bad habits that can lead to a hack and what you can do to reduce your risk.

1. Giving out your e-mail Just about every website wants your e-mail address. If you share it with a vendor or e-commerce site, it's usually not a big deal (though it varies by site – some are more than happy to sell your e-mail to advertisers). The point is that when you share your e-mail, you have no idea where it will end up – including in the hands of hackers and scammers. The more often you share your e-mail, the more you're at risk and liable to start getting suspicious e-mails in your inbox.

If you don't recognize the sender, then don't click it. Even if you do recognize the sender but aren't expecting anything from them and do click it, then DO NOT click links or attachments. There's always a chance it's malware. If you still aren't sure, confirm with the sender over the phone or in person before clicking anything.

2. Not deleting cookies Cookies are digital trackers. They are used to save website settings and to track your behavior. For example, if you click a product, cookies are logged in your browser and shared with ad networks. This allows for targeted advertising.

There's no good way to tell who is

Continued on pg.2

tracking online. But you can use more secure web browsers, like Firefox and Safari. These browsers make it easy to control who is tracking you.

In Firefox, for example, click the three lines in the upper right corner, go into the Options menu and set your Privacy & Security preferences. Plus, every web browser has the option to delete cookies – which you should do constantly. In Chrome, simply click History, then choose "Clear Browsing Data." Done. You can also use ad-blocking extensions, like uBlock Origin, for a safe web-browsing experience.

3. Not checking for HTTPS Most of us know HTTP – Hypertext Transfer Protocol. It's a part of every web address. However, most websites now use HTTPS, with the S meaning "secure." Most browsers now automatically open HTTPS websites, giving you a more secure connection, but not all sites use it.

If you visit an unsecured HTTP website, any data you share with that site, including date of birth or financial information, is not secure. You don't know if your private data will end up in the hands of a third party, whether that be an advertiser (most common) or a hacker. Always look in the address bar of every site you visit. Look for the padlock icon. If the padlock is closed or green, you're secure. If it's open or red, you're not secure. You should immediately leave any website that isn't secure.

> **"Good IT security can be the best investment you can make for the future of your business."**

4. Saving passwords in your web browser Browsers can save passwords at the click of a button. Makes things easy, right? Unfortunately, this method of saving passwords is not the most secure. If a hacker gets your saved passwords, they have everything they could ever want. Most web browsers require a password or PIN to see saved passwords, but a skilled hacker can force their way past this if given the chance.

Protect yourself with a dedicated password manager! These apps keep passwords in one place and come with serious security. Password managers can also suggest new passwords when it's time to update old passwords (and they remind you to change your passwords!). LastPass, 1Password and Keeper Security Password Manager are good options. Find one that suits your needs and the needs of your business.

5. You believe it will never happen to you This is the worst mentality to have when it comes to cyber security. It means you aren't prepared for what can happen. Business owners who think hackers won't target them are MORE likely to get hit with a data breach or malware attack. If they think they are in the clear, they are less likely to invest in good security and education for their employees.

The best thing you can do is accept that you are at risk. All small businesses are at risk. But you can lower your risk by investing in good network security, backing up all your data to a secure cloud network, using strong passwords, educating your team about cyberthreats and working with a dedicated IT company. Good IT security can be the best investment you make for the future of your business.

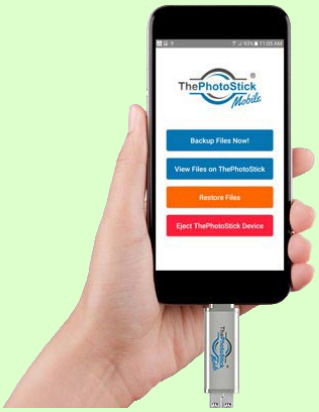
Are Your Digital Credentials For Sale On The DARK WEB?

Visit

www.optistartech.com/darkweb/

For A Free Dark Web Scan!

Shiny New Gadget Of The Month:



ThePhotoStick

Never worry about running out of memory on your smartphone again! It happens to all of us – you're trying to take a picture or record a video and you get a message saying your phone's storage is full. You don't want to buy another new smartphone, so what can you do besides delete old photos?

This is where ThePhotoStick Mobile comes in. It's a memory stick compatible with most Android and iPhone devices and will boost your phone's memory without your having to buy a new phone. ThePhotoStick Mobile is an insurance policy against lost photos and videos.

ThePhotoStick Mobile gives you more control. While most smartphones work without a hitch for years, you never know if something might happen or if you'll run out of memory. ThePhotoStick Mobile plugs into your device and allows you to copy photos over. You can keep them on ThePhotoStick or transfer them to another device. Learn more at GetPhotoStickMobile.io!

Identity Management Solution

Cyber Security, meet Employee Productivity. Employee Productivity, meet Cyber Security. I know you two have not gotten along well in the past, but those days are over.

Cyber criminals are breaching networks worldwide with greater efficiency. The easiest and most effective way they are doing this is by getting ahold of people's passwords. There are many methods criminals use to obtain someone's password. No matter how much awareness training, complex passwords set or network policies implemented, they *still* seem to get their hands on them. One MAJOR deterrent from handing over the keys to your personal data, intellectual property and client information along with a password is the use of **multi-factor authentication (MFA).**

MFA provides a second (or more) check after someone enters their username and password to verify their identity. MFA has become almost ubiquitous nowadays. You see the option when setting up a new iPhone, accessing banking applications, or using a new cloud application. So, why has it not been so ubiquitous in the small and medium enterprise community?

One word: **Convenience**. For the most part, people err on the side of convenience rather than security, even when making business decisions. Owners and leaders want their teams productive. Enduring the hassle of using MFA to gain access to business applications does not usually equate to productivity.

Thankfully, there IS a better way.

Optistar has partnered with DUO, a Cisco company, to provide our clients a seamless and secure solution for accessing cloud applications and critical business applications.

Our Identity Management Solution incorporates both **single sign on (SSO)** to conveniently access applications with a single username and password and **multi-factor authentication** to add an extra layer of security to them.

Our managed MFA solution, through DUO, provides an easy-to-use, secure mobile authentication app for quick, push notification-based approval to verify your user's identity with smartphone, smartwatch and U2F token support.

SMS-based two-factor authentication is no longer considered secure by the National Institute of Standards and Technology (NIST) standards, as SMS messages can be easily intercepted or redirected by remote attackers. Using an authentication app, users can log in with their primary credentials, and then their app will prompt them with a push notification to complete the secondary authentication by approving the request. This method is more difficult for attackers to intercept and offers a convenient way for users to log in by using their smartphone or other device.

Our fully managed solution includes:

- Single Sign On (SSO) to your business Cloud Apps
- Integrated MFA solution
- A centralized dashboard to all your business apps
- Implementation and management of all MFA and SSO policies
- Quarterly security review
- Authentication logs reviewed and saved for 7 years
- DUO subscription for each of your employees
- Unlimited Support for each of your employees

Call us today at 888-782-7003 to learn more!

147 West 35th Street, 19th FL
New York,, NY 10001

Optistar Technology Consultants has been providing expert Information technology advice, help and services to small and medium businesses since 1996.

Most of our clients hire us to support their network because they do not want to incur the overhead and cost of full time IT staff and they do not want to burden their employees with the responsibility of troubleshooting the company network.

For over 20 years, Optistar has built a reputation for providing superior strategic IT consulting and solutions for its customers which has set us apart from the typical computer consultant and other providers.

Need help or have a question? Call us at 888-782-7003 or shoot us an email at ask@optistartech.com

"You know, you think after a while you'd get tired of profits. But I just never do."