1991 – 2021
30 YEARS OF EXCELLENCE
Computer Technologies, Inc.

TECHNOLOGY TIMES

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

What's Inside

September 2022

Kim Nielsen
President & Chief Technology Strategist at Computer Technologies Inc.
(248) 362-3800

"As a business owner, you don't have time to waste on technical and operational issues. That's where we *shine*! Call us and put an end to your IT problems finally and forever!"

Honesty Is the Best Policy…Even When You're Being Hacked

When a data breach goes public, especially if the affected company kept it a secret from the people who use their services, the resulting outcry can have a negative impact on the victim's reputation. Keeping threats and breaches quiet only cause customers to lose trust in the company's ability to keep their PII safe. Think about it: Remember the data leak that exposed Uber's database of names, addresses and driver's licenses for riders and drivers alike? A cybersecurity breach costs more than the initial damage: Users may opt to switch services, your investors could pull out and recuperation or litigation fees can really pile up.

It's understandable why cases like Uber didn't want to announce to the public that they'd been hacked. Instead, they discreetly paid off the ransomware and users of the app didn't find out for a year that their information had been compromised. Waiting for the cat to let itself out of the bag prevents customers from taking their own security measures with their accounts as they see necessary. Ultimately, it does even more damage than facing the consequences upfront.

When it's time to own up to a data breach or loss, businesses fare best when they're open and honest with their customers about the event from start to finish. Here's why.

The Risks of Keeping Quiet

No one likes to feel as though important information has been hidden from them, for any length of time. Customers are the same. When they're kept abreast of a breach, what the company is doing to remove the intruder and recover data, and post-attack recovery efforts, customers can trust you to protect and inform them in the future. Instead of wondering all the

Continued on pg.2

Continued from pg.1

time if they need to change their passwords, they'll know for sure when it's necessary. They also feel comforted knowing the steps you're taking to recover data and patch the vulnerabilities are effective, or can take their own additional precautions, when you're open about the steps being taken to combat the threat.

Well aside from the risk you run of pushing away customers with silence, there may also be legal repercussions at stake. For example, banks are experiencing cybersecurity reform that requires them to report breaches, data corruption and the like **within 36 hours**. As more people, industries and governments turn their attentions toward better cybersecurity systems, it is likely that there will also be more legislation written to support cybersecurity for our critical infrastructures (like The Cybersecurity Act of 2021) or to invest in technology that will change the industry altogether.

"That Can't Possibly Work!"

If you're still feeling inclined to keep breaches a secret from your client base, consider that other organizations have already made that difficult announcement and you can see what these "guinea pigs" uncovered.

Corporations like Microsoft, Google and Apple – whom you expect to keep your most sensitive online data locked tight – have all disclosed breach incidents in the past few years. This only goes toward normalizing the high probability of cyberattacks given how advanced these threat tactics have become. As it turns out, customers prefer this route.

- Knowing real-time information about the hack and its patches allows customers to make the best decisions about their own accounts
- They can trust that you will disclose attempted hacks in the future, thereby feeling more secure in your hands around the clock
- Disclosures about how you're going about fixing the breach and preventing it from ever happening again give them more education and knowledge about cyber-threats and -security, helping to prevent future hacks on their devices.

Even notifying users about vulnerabilities detected and patched before the software has been launched helps build brand loyalty.

People appreciate straightforwardness, as long as the underlying effort is there. Being truthful about attempted or successful cyberattacks garners more support than vitriol for your brand.

Conclusion

You already have so much to think about when a breach is discovered in the company network. What to do, who to tell and what protocol to follow are all swimming around your mind. Instead of shying away from your loyal base, take the opportunity to lean on your support network through tough times, while simultaneously reassuring them about how you're working to recover and protect their most sensitive data.

Cyber threats are a danger to your business as well as the customers who trust you. Encrypting and backing up data regularly, to a safe place of storage that's easily accessible to you, can protect sensitive information from cybercriminal activity. When threats do happen, an open and honest policy will help to preserve your positive customer relationships.

Free Cyber Risk Audit Will Reveal Where Your Computer Network Is Exposed And How To Protect Your Company Now

At no cost or obligation, our highly skilled team of IT pros will come to your office and conduct a comprehensive cyber risk audit to uncover loopholes in your company's IT security.

After the audit is done, we'll prepare a customized "Report Of Findings" that will reveal specific vulnerabilities and provide a Prioritized Action Plan for getting these risk problems addressed fast. This report and action plan should be a real eye-opener for you, since almost all of the businesses we've done this for discover they are completely exposed to various threats in a number of areas.

Claim Your FREE Assessment Today At:

https://www.cti-mi.com/cyber-security-audit922/

Or Call Our Office At: 248-362-3800

Security Corner

Don't Settle For Notes App Passwords: Get A Manager Instead

Hard-to-guess passwords are essential to protecting your accounts and they should include a mix of letters, numbers and symbols. They also shouldn't spell out anything that's easy to attribute to you, thus giving hackers an easy time guessing your account credentials.

Remembering complex passwords can be…complex.

Maybe you've solved this conundrum a simple way, like cutting and pasting a list in your notes app or keeping a journal locked up in your desk. Unfortunately, writing down your account credentials, whether digitally or physically, creates opportunities for a thief to get their hands on it. That's why many people use a password manager instead.

A Password Manager can do many things including:

- Safely store ALL your credentials
- Retrieve and fill in your account information with the press of a button
- Prompt you to change insecure passwords

One thing to keep in mind is that your Master Password — the one that gets you into your Password Manager of choice — can't match any of the ones locked in its vault. Why? If a hacker gets control of an account that shares the password, but which is less secure, then they could potentially break into your entire storage of saved credentials.

For more information about email security, call us at 248-362-3800 or visit: https://bit.ly/3QHYgJu

You Need To Watch Out For Reply Chain Phishing Attacks

Phishing. It seems you can't read an article on cybersecurity without it coming up.

That's because phishing is still the number one delivery vehicle for cyberattacks.

80% of surveyed security professionals say that phishing campaigns have significantly increased post-pandemic.

Phishing not only continues to work, but it's also increasing in volume due to the move to remote teams.

Many employees are now working from home. They don't have the same network protections they had when working at the office.

One of the newest tactics is particularly hard to detect. It is the reply-chain phishing attack.

What is a Reply-Chain Phishing Attack?

You don't expect a phishing email tucked inside an ongoing email conversation between colleagues.

Most people are expecting phishing to come in as a new message, not a message included in an existing reply chain.

The reply-chain phishing attack is particularly insidious because it does exactly that. It inserts a convincing phishing email in the ongoing thread of an email reply chain.

How does a hacker gain access to the reply chain conversation? By hacking the email account of one of those people copied on the email chain.

The hacker can email from an email address that the other recipients recognize and trust. The attacker also gains the benefit of reading down through the chain of replies. This enables them to craft a response that looks like it fits.

They may see that everyone has been weighing in on a new product idea for a product called Superbug. So, they send a

reply that says, "I've drafted up some thoughts on the new Superbug product, here's a link to see them."

The reply won't seem like a phishing email at all. It will be convincing because:

• It comes from an email address of a colleague. This address has already been participating in the email conversation.

• It may sound natural and reference items in the discussion.

• It may use personalization. The email can call others by the names the hacker has seen in the reply chain.

Business Email Compromise is Increasing

Business email compromise (BEC) is so common in the business world that it now has its own acronym.

Weak and unsecured passwords lead to email breaches. So do data breaches that reveal databases full of user logins.

Tips for Addressing Reply-Chain Phishing

Here are some ways that you can lessen the risk of reply-chain phishing within your own organization:

• Use a Business Password Manager

• Put Multi-Factor Controls on Email Accounts

• Teach Employees to be Aware

Reduce Risk When You Lose A Mobile Device

Few things invoke instant panic like a missing smartphone or laptop. These devices hold a good part of our lives.

This includes files, personal financials, apps, passwords, pictures, videos, and so much more.

The things you do in the minutes after missing a device are critical. This is the case whether it's a personal or business device. The faster you act, the less chance there is for exposure of sensitive data.

Steps to Take Immediately After Missing Your Device

• Activate a "Lock My Device" Feature

• Report the Device Missing to Your Company

• Log Out & Revoke Access to SaaS Tools

• Log Out & Revoke Access to Cloud Storage

• Active a "Wipe My Device" Feature

6 Important IT Policies Any Size Company Should Implement

Many smaller businesses make the mistake of skipping policies. They feel that things don't need to be so formal.

But this way of thinking causes issues for business owners. Employees aren't mind readers.

Things that you think are obvious, might not be to them. IT policies are an important part of your IT security and technology management. Here are some of the most important to have in place.

1. Password Security Policy
2. Acceptable Use Policy (AUP)
3. Cloud & App Use Policy
4. Bring Your Own Device (BYOD) Policy
5. Wi-Fi Use Policy
6. Social Media Use Policy

Technology Tools You Should Uninstall

While older technology may still run fine on your systems that doesn't mean that it's okay to use. One of the biggest dangers of using outdated technology is that it can lead to a data breach.

Outdated software and hardware no longer receive vital security updates and patches. No security patches means a device is a prime target for a cyber security breach.

Get Rid of This Tech Now If You're Still Using It:

- Internet Explorer
- Adobe Flash
- Windows 7 and Earlier
- macOS 10.14 Mojave and Earlier
- Oracle 18c Database
- Microsoft SQL Server 2014 (losing support in 2024)

"I just feel fortunate to live in a world with so much disinformation at my fingertips."

CartoonStock.com