Talk Nerdy To Me

1

February 2020

FBI Warns of New Online Threat to Personal Credit Card Information

Never using a debit card online and asking a company for a virtual credit card are among steps that consumers can take to protect themselves.

Federal authorities have a consumer warning for shoppers. Hidden skimming devices (commonly thought to be attached to gas station pumps and ATMs) have gone high-tech. “It’s hard to put really — definite numbers around it. But one thing we know for sure is that millions of credit card numbers have been stolen, even over the course of the past two years,” Herb Stapleton, section chief for the FBI’s cyber division told CNBC. This new type of skimming is called e-skimming or Magecart.

Cybercriminals can gain access to your personal and credit card information in a number of ways. They can break into a web server directly or break into a common server that supports many online shopping websites to compromise them all and once a site has been compromised, the shopper can’t spot the difference.

“It’s nearly impossible for a consumer to detect that this has happened to them before the actual occurrence. The site that they would look at, which is already infected, would look no different to a consumer,” Stapleton said.

Randy Pargman is the senior director for threat hunting and counterintelligence at Binary Defense, an Ohio-based cybersecurity company that monitors companies’ computers for signs of attacks. The company won’t disclose its clients but says many are in the retail sector.

Victims of e-skimming include Macy’s, Puma’s Australian website, Ticketmaster’s United Kingdom website and British Airways. The companies did not respond to requests for comment.

“Any retailer that has a significant online presence that accepts online orders is definitely concerned about e-skimming,” Pargman said. For consumers, there are several things you can do to protect yourself when shopping online.

1. Always shop with a credit card instead of a debit card online. This lessens the inconvenience if your card is compromised, Pargman said. Credit card users usually have a lower liability for fraud. In addition, getting money returned to your debit card can take some time.

2. Consider asking your bank or credit card company for a virtual credit card. Not all banks offer it but many do. The virtual credit card is a unique credit card number to be used for specific transactions and for a specific merchant. If this number is compromised, other charges will be declined.

3. Monitor their cards for any unusual activity and report it right away.

While the FBI’s Stapleton said e-skimming has been on its radar for nearly seven years, he said the crimes are growing because cybercriminals are sharing the malware online and becoming more sophisticated.

“If we put up a wall,” Stapleton said, “they’re building a ladder or a tunnel or a way to go around it.”

Source: CNBC.com

February 2020

Big Microsoft Data Breach 250 Million Records Exposed

Microsoft has announced a data breach that affected one of its customer databases. Between 05 December 2019 and 31 December 2019, a database used for "support case analytics" was effectively visible from the cloud to the world.

Microsoft didn't give details of how big the database was. However, consumer website Comparitech, which says it discovered the unsecured data online, claims it was to the order of 250 million records containing:

…logs of conversations between Microsoft support agents and customers from all over the world, spanning a 14-year period from 2005 to December 2019.

According to Comparitech, that same data was accessible on five Elasticsearch servers. The company informed Microsoft, and Microsoft quickly secured the data.

Microsoft's official statement states that "the vast majority of records were cleared of personal information," meaning that it used automated tools to look for and remove private data.

However, some private data that was supposed to be redacted was missed and remained visible in the exposed information.

Microsoft didn't say what type of personal information was involved, or which data fields ended up un-anonymised.

It did, however, give one example of data that would have been left behind: email addresses with spaces added by mistake were not recognised as personal data and therefore escaped anonymisation.

So if your email address were recorded as "name@example.com" your data would have been converted into a harmless form, whereas "name[space]@example.com" (an easy mistake for a support staffer to make when capturing data) would have been left alone.

Microsoft has promised to notify anyone whose data was inadvertently exposed in this way, but didn't say what percentage of all records were affected.

What to do?

We don't know how many people were affected or exactly what personal data was opened up for those users.

We also don't know who else, besides Comparitech, may have noticed in the three weeks it was exposed, although Microsoft says that it "found no malicious use".

We assume that if you don't hear from Microsoft, even if you did contact support during the 2005 to 2019 period, then either your data wasn't in the exposed database, or there wasn't actually enough in the leaked database to allow anyone, including Microsoft itself, to identify you.

It's nevertheless possible that crooks will contact you claiming that you *were* in the breach. They might urge you to take steps to "fix" the problem, such as clicking on a link and logging in "for security reasons", or to "confirm your account", or on some other pretext.

Remember: if ever you receive a security alert email, whether you think it is legitimate or not, avoid clicking on any links, calling any numbers or taking any online actions demanded in the email. Find your own way to the site where you would usually log in, and stay one step ahead of phishing emails!

Source: https://nakedsecurity.sophos.com/

BEFORE THE BREACH

HACKERS ARE HERE!

NEW SKILLS FOR A NEW FIGHT

- 1 in 5 businesses will suffer a cyber breach this year
- 81% of all breaches happen to small/medium sized businesses
- 66% of companies do NOT test their backups
- 60% of companies that lose their data will go out of business within 6 months
- 92% of malware is delivered via email
- 97% of breaches could have been prevented with today's technology

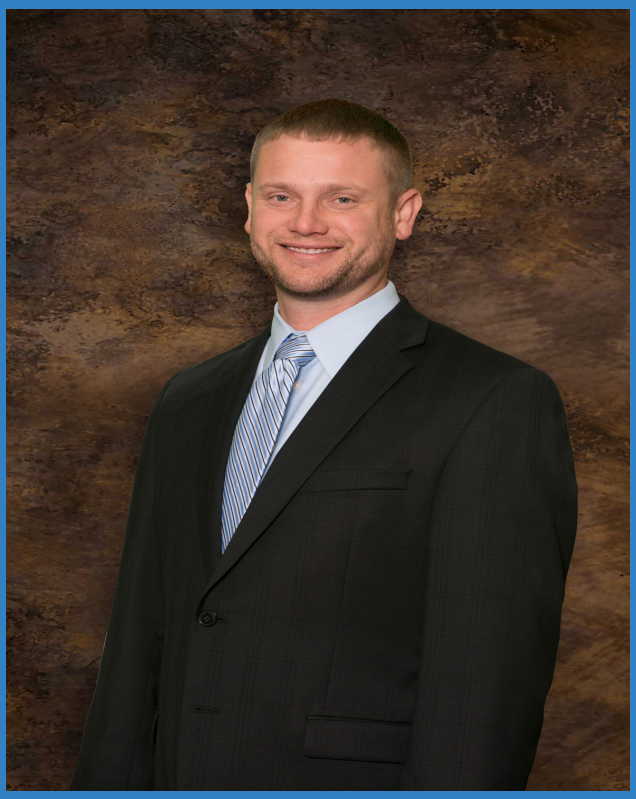
Want to learn more about how to protect your business?

Stay tuned for our next lunch and learn date!

www.preferreditgroup.com/beforethebreach

talk nerdy to me

PREFERRED IT EMPLOYEE SPOTLIGHT



Meet Jason Horne! He is the owner and CEO of Preferred IT Group. He founded Preferred IT Group, LLC. with his former business partner over 15 years ago. He realized early on that managed IT services was the niche we wanted to be in and we've based and grown our company on that model ever since.

Jason recently completed a course with Harvard University in Cybersecurity: Managing Risk in the Information Age. He is committed now more than ever, to providing our customers with the knowledge and peace of mind needed to protect themselves from ever growing cyber threats.

In Jason's free time, he enjoys doing outdoor activities like hunting, fishing, snowboarding and golfing. He enjoys music and plays the guitar. Jason married his highschool sweetheart and will be celebrating 19 years of marriage this year! He is also very involved with his 3 kids, coaching softball and football and being a supportive dance dad!

Our Promises To You!

When you call Preferred IT Group, you will speak with a team member when you call!
You will not enter into a call center or be forced to listen to menu options. During business hours, we answer every call live!

We will answer the phone with a smile!
You're already having technology issues and we want you to know we will takle them with a can-do, positive attitude.

We will communicate with you in terms you understand!
No geek speak is very important to us. We want to make sure we communicate effectively from start to finish.

We will tailor our solutions to you needs!
We have different levels of management to choose from as well as extra services that can be added based on what your company wants.

We strive to provide a one call resolution!
When you call in an issue, we want to double and triple check that the issue is resolved and that you're satisfied.

TOP 3 IT IN FORT WAYNE

Did you hear the news?!
Preferred IT Group, LLC. was named as one of the top 3 IT companies in Fort Wayne by threebestrated.com!

If your business is looking for outstanding customer service and expert knowledge, give us a call today!

preferred IT group

CONTACT US

Fort Wayne
260.440.7377
Warsaw
574.306.4288
Columbia City
260.213.4266
Indianapolis
317.426.8180

www.preferreditgroup.com

6333 Constitution Drive
Fort Wayne, IN 46804

Subscribe to our blog and follow us on social media.