Cybersecurity Is A Big Concern

Marriott hacked 5.2 million guests

Bad actors accessed a range of personally identifiable information a lot more

Amer Owaida 1 Apr 2020 - 04:42PM

Honda Hit by Ransomware: Attack Follows Major 2019 Data Breach

At this time Honda Customer Service and Honda Financial Services are experiencing technical difficulties and are unavailable. We are working to resolve the issue as quickly as possible. We apologize for the inconvenience and thank you for your patience and understanding.

101 12:48 - 8 Jun 2020

136 people are talking about this

The company's Twitter feed shows that both Honda Customer Service and Honda Financial Services, the company's lending arm, are "experiencing technical difficulties and are unavailable".

Customers facing issues with their vehicles are being urged to DM their full name, VIN, mileage, address, email, best contact number and other details through Twitter. Additionally, Honda dealers are being directed to a webpage with frequently asked questions.

Honda Automobile Customer Service via Twitter
"The average company handles a bombardment of 200,000 security events a day"

89% of companies say they have been the victim of a cyber attack in the last 12 months. 1 in 3 say they have been hacked more than 5 times in the past year.

"Only two types of organizations: Those that know they have been attacked, and Those that don’t YET know that they have been attacked."

- Professor Stuart Madnick

Source: Harvard Business Review, "Cybersecurity has a serious talent shortage and here’s how to fix it". Posted online May 4, 2017
COVID-19 Has Created the Perfect Storm of Fear, Uncertainty, Doubt (FUD) and Chaos

The bad guys have upped their game.
We have to do the same

As we all work from home, keeping ourselves, our families and our organization safe has never been more urgent and important

1. Technology (firewalls, spam collectors, etc) cannot keep us 100% secure
2. 90+% of breaches start with some type of ‘human error’
   → Phishing emails (fraudulent email sent to trick you into inappropriate action)
   → Fake websites (websites with fake info, bad links, or phony offers)
   → Bad files (pdf, xls, etc with extra code embedded in them)
3. The current pandemic has been accompanied by a major increase in cyber crime


©2020 Keri Pearlson and Cybersecurity at MIT Sloan (CAMS). All Rights Reserved. For copies or to use any of these materials, please contact kerip@mit.edu
Email Scams During Pandemic

- WHO email with Safety measures (see copy on this slide)
- CDC email: ‘updated new cases in your city’ messages (asks for information and login credentials)
- Emails purportedly about government stimulus checks asking you for information
- Business email spoofing: emails look like they come from someone in your company and ask you to do something like click on a link or wire money to a fake account


©2020 Keri Pearlson and Cybersecurity at MIT Sloan (CAMS). All Rights Reserved. For copies or to use any of these materials, please contact kerip@mit.edu

Information Stealing and Social Engineering Scams

A file has embedded code in it that gets planted on your system (malware)

Example: Coronavirus Map (see image on this page)

-- this map is weaponized with malware code written into it

-- Steals user name, passwords, bank account numbers, credit card numbers and other sensitive and personal data stored in a browser.


©2020 Keri Pearlson and Cybersecurity at MIT Sloan (CAMS). All Rights Reserved. For copies or to use any of these materials, please contact kerip@mit.edu
Ransomware and Blackmail Attacks

Ransomware is when the malicious actors steal data from a company and/or lock up the systems/laptops and hold the owner hostage for payment

Ex: NetWalker is using a file it created called “CORONAVIRUS_COVID-19.vbs”. Sounds like something important, but actually puts code on machine that encrypts files then displays note (see image on this slide)

You are asked to follow instructions to get your files and system back (and sometimes that won’t even fix things)


©2020 Keri Pearlson and Cybersecurity at MIT Sloan (CAMs). All Rights Reserved. For copies or to use any of these materials, please contact kerip@mit.edu

Working From Home Vulnerabilities

-Webinar software hack: We are seeing uninvited guests log into Zoom meetings (Zoom Bombing).

-Mixing networks: We are seeing workers at home using the same network as children at ‘virtual school’ and family members playing/surfing the net.

-VPNs: We are seeing compromises to company-managed VPNs. Be sure you have the latest security for your access to your company VPN

©2020 Keri Pearlson and Cybersecurity at MIT Sloan (CAMs). All Rights Reserved. For copies or to use any of these materials, please contact kerip@mit.edu
Fake Pharmacies and Remedies

- Increased number of spam campaigns using fake news about virus-preventing meds/remedies
- Designed to spread malware or get you to spend money (but not deliver anything for it). This is called “clickbait” - hackers try to get you to click on something.
- Best case is just to increase SEO of other questionable sites

June 27, 2020: Fake Face Mask Exempt Cards

The card shows the U.S. Justice Dept logo and says:

“Wearing a face mask poses (sic) a mental and/or physical risk to me. Under the Americans with Disability Act (ADA), I am not required to disclose my condition to you.”

CAMS Research: Building a Culture of Cybersecurity

How can we create a culture of cybersecurity in our organizations (like our culture of safety)?

Our research suggests that changing values, attitudes and beliefs is the key to creating cybersecure behaviors.

MIT Research: Build Values, Attitudes and Beliefs to Drive Secure Behaviors

MIT Cybersecurity Culture Model

For more information: https://cams.mit.edu/research
To Summarize:
Some Things to Look Out For

Calls, emails or texts about government stimulus, COVID-19 remedies, or anything asking for SSN or other personal information

Online ads for masks, ppe, test kits, vaccinations, medicines, and other things we are seeking during COVID-19. Make sure anything you buy is from a reputable source

Demands for payment from utility company, phone company, internet company, bank/credit card company, etc. All of these kind of requests must be verified before you send any money to anyone.

Emails or calls from coworkers or company officials that you did not expect. Contact them separately (do not just ‘reply’ to the email) to verify.

Call to Action: What You Can do Today to Help Protect Your Family and Your Organization

1. Make sure your laptop, cell phone and apps are up to date (install all patches, updates, etc. Many are designed to fix vulnerabilities)
2. Protect your key assets (bank account/credit cards). Change your passwords. Use dual authentication where you can. Check your email here to see where it’s been compromised (https://haveibeenpwned.com).
3. Do not click on emails or websites that you do not know well. If you do, contact your IT support immediately so they can tell you what to do next.
4. Model the values, beliefs and attitudes you want from those around you. Make heroes out of those who do things to protect digital assets. Show them it’s one of your priorities and it will become important to them too.
5. Share ideas with your family, friends and coworkers. Bring the issue out in the open and discuss it…the bad guys thrive on FUD and chaos (and COVID19 has all of this)
6. Keep aware of the latest breaches so you know if you are affected

©2020 Keri Pearlson and Cybersecurity at MIT Sloan (CAMS). All Rights Reserved. For copies or to use any of these materials, please contact kerip@mit.edu
Our Research Group: Cybersecurity at MIT Sloan (CAMS)

Our strategic objective: Raise the cybersecurity level of all organizations (public/private, big/small, global/domestic).

We research the fundamental issues of cybersecurity strategy, leadership and management.

We are funded by companies like yours.

For more information:
https://cams.mit.edu/

©2020 Keri Pearlson and Cybersecurity at MIT Sloan (CAMS). All Rights Reserved. For copies or to use any of these materials, please contact kerip@mit.edu

THANK YOU!

Check out our Cybersecurity for Executives (online or in person) Executive Education Programs at https://executive.mit.edu/

More info available at: https://cams.mit.edu or contact me at: kerip@mit.edu