

WELCOME



Cyber Security Basics for E-commerce

Wednesday, March 9, 2022



This webinar is offered in partnership between Tourism Nova Scotia and Digital Nova Scotia through DigiPort, a one-stop-shop of interactive services and educational opportunities to help tourism businesses develop digital marketing skills and access professional support to improve their online presence.

Sign up for Digiport at
<https://nsdigiport.ca/>



Digital Support for
Nova Scotia's Tourism Sector

Sign up

Get in touch with our network of digital marketing strategy experts.

PRESENTER

arbuckle.media

Joel Arbuckle

- Joel is the President of Arbuckle Media, which he founded in 2015.
- Arbuckle Media is a digital branding agency, raising businesses up using powerful social media creative campaigns and powerful branding executions.
- Joel's favourite projects are the ones with the opportunity to take inspiration from the current trends that major international brands are using, analyze the nuts and bolts of why they work, and create a blueprint from the same principles that yields results for the little guys.
- Joel says the things he loves most about growing his business in Nova Scotia are the amazing people, communities and brands, as well as the virtually unlimited potential he sees all around him.

Cybersecurity Basics for E-commerce

With Joel Arbuckle

Outline of this Exercise

This *isn't* designed to be an in-depth analysis of any particular type of spam, scam, attack.

This *is* designed to produce awareness of all the different types of attacks and how a simple, cost-effective list of best practices and standards within your organization can cover many bases at once, and likely save you a lot of pain and frustration should you become the subject of an attack.

Why: why bad actors typically attack small business websites

How: types of attacks, what to look for, how to know when you're under attack

What to do before, during and after an attack has taken place

Prevention methods: how to prevent your business from becoming a victim of these vicious, anonymous attacks.

Basic steps to follow during and after an attack; and

Policies and procedures you can put in place with your staff and team in order to prevent the spread of threats

Why Small Businesses?



You May Ask Yourself: “Why Me?”

Often those who are attacked (especially small businesses) think they aren’t of interest to bad actors. **Wrong.**

◆ **43% of cyber attacks target small businesses**, and that trend seems to be increasing YoY.

Any information or records you have is valuable.

Additionally, you could often be a *secondary target*.

E-commerce is especially vulnerable and under fire because of its proximity to your customers’ personal financial information.

Hackers and bad actors know the unfortunately, for many small businesses **cybersecurity is still an afterthought.**

Consumers expect that their privacy and confidential information will be protected. It’s every consumer’s right to demand security from the companies they do business with.

Basic Types of Attacks



Basic Types of Attacks

A non-exhaustive list of the most common types we've seen impact users and businesses locally:

- Phishing (aka social engineering)
- Carding or Card Testing
- Password or 'Brute Force' Attack
- Malware
- DDoS/DoS
- Internet of Things (IoT) Attacks

Phishing (or Social Engineering)

Likely the most common attack you'll see as a small business.
a type of fraud and social engineering that comes in many forms

They want to trick you, your employees, or even your grandmother into thinking they are who they say they are.

The most common types of phishing are:

- ◆ **Spear Phishing** — targeted attacks directed at specific companies and/or individuals.
- ◆ **Whaling** — attacks targeting senior executives and stakeholders within an organization.
- ◆ **Pharming** — capturing user credentials through a fake login landing page.

Liability: lose control of everything, and often leveraged to carry out a MitM attack



Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: \$135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

<http://www.trustedbank.com/general/custverifyinfo.asp>

Once you have done this, our fraud department will work to resolve this discrepancy. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.





Carding or Card Testing


Carding or card testing is the testing of stolen credit card or financial and banking information against your system to either get 'free' (to them) product(s) from your business, or more often, find out what credit card info in their possession is still working.

How to spot it: a number of credit cards being run in a short period of time for the same or similar products.

Liability: This can result in your organization incurring chargebacks, being subject to investigation by law enforcement, and even compromising the relationship between you and your payment processors.


Payment
All transactions are secure and encrypted.


☒ Credit card     and more...


Card number 

Name on card

Expiration date (MM / YY)

Security code 

☐ 

☐ 

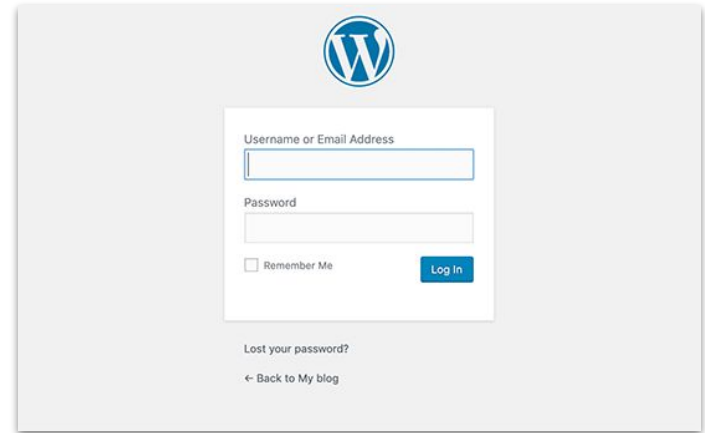
Brute Force & Password Attacks

Another very common type of attack.

The password attack or brute force attack is a barrage of attempts to login to your accounts.

Because of the nature of the attack, it's easy to limit and block the number of attempts from a bad actor on this one.

Liability: compromised accounts, and loss of control of important assets or accounts.



Malware

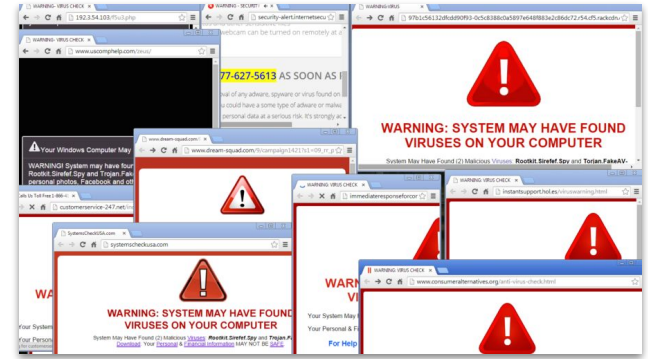
The term “malware” includes spyware, viruses, and worms.

Malware can:

- ◆ Deny access to the critical components of the network
- ◆ Obtain information by retrieving data from the hard drive
- ◆ Disrupt the system or even render it inoperable

Liability: Malware attacks are often leveraged to carry out

Pharming (Phishing) and other MitM attacks, and do damage to not only your systems and hardware, but also your customers’ hardware as well.



DDoS/DoS

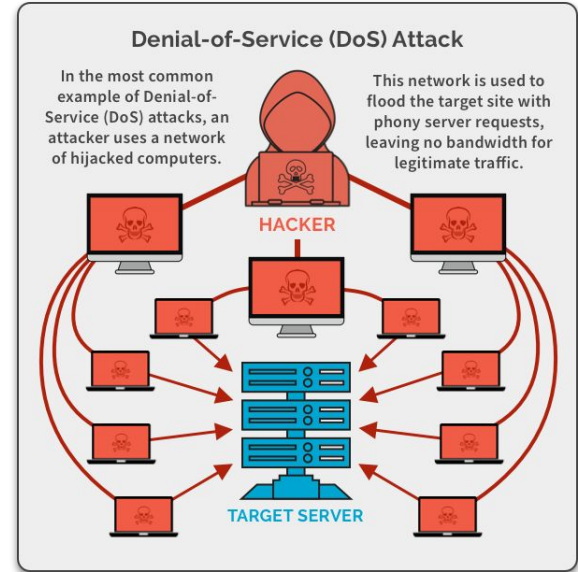
A DoS attack is a denial of service attack where a computer is used to flood a server with traffic.

DDoS attacks can come in various forms, some of which are:

- ◆ Buffer overflow attacks
- ◆ Ping of Death

DoS are easy to coordinate.

Liability: They can hurt your infrastructure, cost you money, and even damage the relationship between your company and your hosting provider, on top of the opportunity cost of your network or website being taken down.



Internet of Things (IoT) Attacks

Do you have a location such as a restaurant or taproom? Perhaps even a lounge or seating area for customers clients?

Do you public wifi available or allow others to use your wifi? Do you have smart devices such as a POS system or consumer electronics used in your organization?

All of the above are significant liabilities to your security.

Liability: Hardest to defend against, although usually requires attackers to be in physical proximity to your business.



Prevention Methods



“So, what do I do?” Prevention Methods

General Rules:

If you make it hard for them, they will likely move on. There are so many businesses out there for them to target, that they won't want to waste time on yours if you don't make it easy for them to do their dirty work.

The easiest way to minimize your risk is to create a system that is thorough, rigid, and enforced without exception. Assume that websites, or any touchpoint of technology you have, is a liability and inherently insecure.

1. Do not store hard text records of any **login credentials**.
2. **Use VPNs** wherever possible, especially if you're using a device that has access to your business' accounts or information while not on your home networks.
3. Create and identify key stakeholders who will act as the “**response team**.”
4. Do not require regular password changes.
5. Educate yourself.

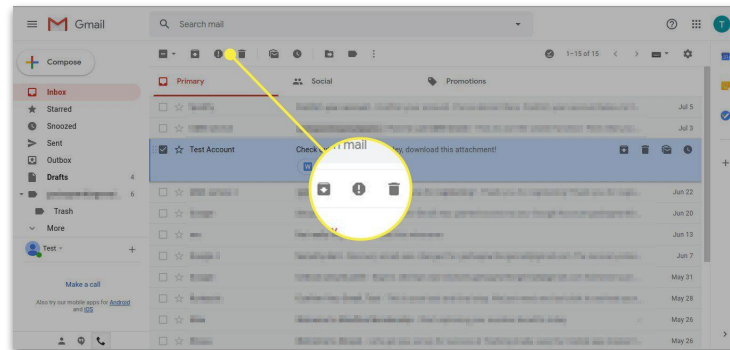
Websites are inherently fragile, and should always be treated like they are not secure.
Everything that is connected to anything is a vulnerability.

Phishing Prevention

Raise awareness within your organization. Share resources, latest phishing new updates.

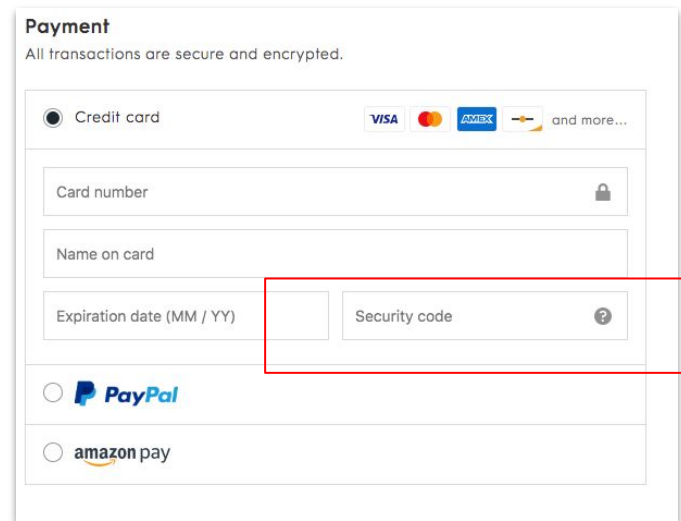
1. Don't click on links or files.
2. Don't be tempted by pop-ups
3. If you get a strange link or file, report it back to the 'real' sender.
4. Get free anti-phishing add-ons and spam filters on your email account and website forms.

Test your team members. Look for weak links in your organization.



Carding or Card Testing Prevention

1. Implement **CVV verification**. Ensure that users must be logical, factual tests when attempting to run their credit card or financial information for payment.
2. Use **postal code match** features during checkout.
3. Rate and velocity IP limiting to restrict the number of checkout attempts in a short period of time.
4. **Set up alerts with your e-commerce engine to receive emails for orders. Review orders when they come in quick succession.**
5. **Work with your payment processor** to create blacklists, and setup monitoring and alerts for fraudulent transactions in realtime.



The image shows a 'Payment' form with the heading 'Payment' and a subtext 'All transactions are secure and encrypted.' Below this, there is a section for 'Credit card' with logos for VISA, MasterCard, AMEX, and Discover. The form includes input fields for 'Card number', 'Name on card', 'Expiration date (MM / YY)', and 'Security code'. A red rectangular box highlights the 'Security code' field, which has a question mark icon next to it. Below the credit card section, there are radio buttons for 'PayPal' and 'amazon pay'.

Brute Force & Password Attack Prevention

1. Do require **strong, secure passwords** on all accounts *and* devices.
2. Use different passwords for every single login you have. No exceptions.
3. Rate and velocity limiting.
4. Blacklist country IPs.
5. Use **multi-factor authentication** (aka 2-factor authentication) wherever and whenever possible.
6. Use a password manager.



Malware Prevention

1. Frequent backups;
2. Constant updating;
3. Firewall and anti-virus software and scanning;
4. Always use premium plugins, etc. for any purpose;
5. Install a Security specific Plugin.



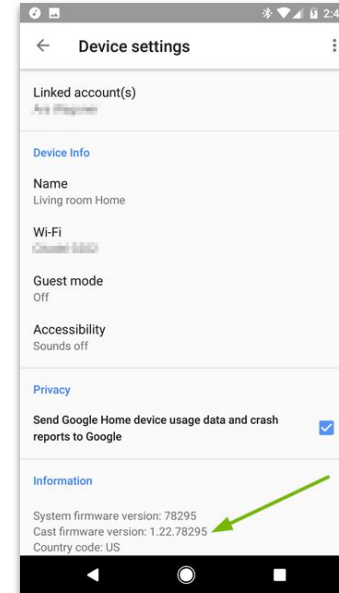
DDoS/DoS Prevention

1. Continuous Monitoring of Network Traffic
2. Consider temporarily offlineing the website or disconnecting the network from the internet during an attack.
3. Web security tools that remove web-based threats, block abnormal traffic, and search for known attack signatures.
4. Use **Cloudflare** as your nameserver to host your DNS settings.



Internet of Things (IoT) Prevention

1. Keeping devices up to date;
2. keeping a strong password for every IoT device on your network, including your home and business wifi networks;
3. using only the least amount of devices you absolutely need.



Prevention Policies & Procedures

1. Create a policy that governs how to protect data and keep accounts and assets secure within your organization.
2. A policy should cover:
 - ◆ Key personnel and 'response team' and roles
 - ◆ Confidential Data
 - ◆ Personal & Company Devices
 - ◆ Emails
 - ◆ Password Management
 - ◆ Multi-factor authentication
 - ◆ Sharing Data
 - ◆ Remote Access

**Review the policy with your team regularly.
Follow it yourself without exception.**

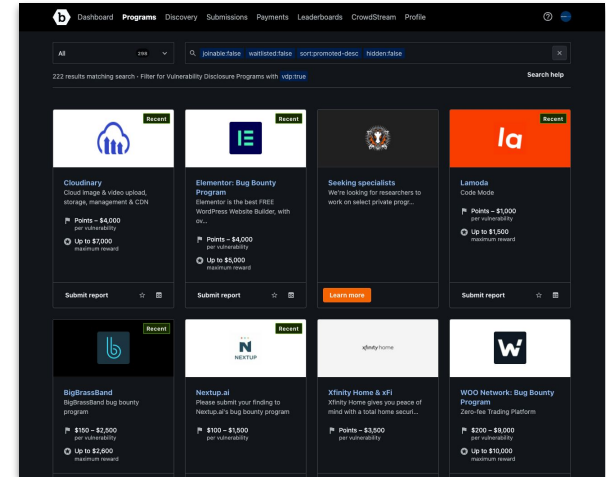


Pay People To Attack You

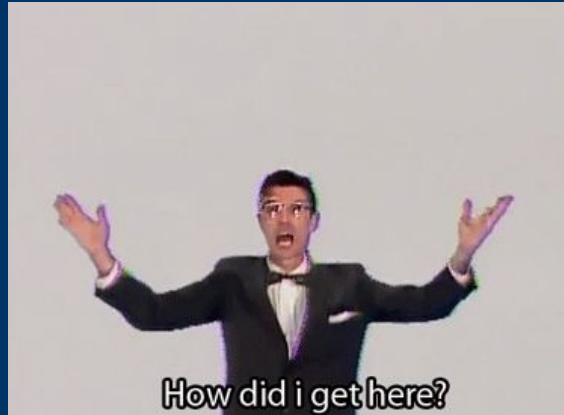
This is not an advisable step for every small business out there, as you will likely deal with unscrupulous actors and people with a deeper understanding of your systems than you do.

→ If you are confident you have a good system setup and feel confident in your position, *and* you can afford it, **pay bug bounties**.

Pay people, whether with money or products, etc., to attempt to run your systems through the wringer, to phish your people.



During & After an Attack



Basic Steps: During & After An Attack

1. Assume the worst, and **trust nothing**. Beware the “backdoor.”
2. Mobilize Your **Cybersecurity Response Team**
3. Identify the Type of Attack, *if possible*
4. **Turtle**: Contain the Breach
5. **Assess** and Repair the Damage, *if possible*
6. **Report** the Attack
7. **Communicate** with Customers
8. **Learn** from the Experience

Plan outline & checklist

- ❑ Ensure Policies are written and established;
- ❑ Define your team members and roles;
- ❑ Inventory all your assets, accounts, hardware and software.
- ❑ Put in place controls and prevention methods.
- ❑ Define the steps in a checklist that will help during an attack.
- ❑ Review with your team the plan;
 - ❑ Familiarize yourself and your team with late articles on cybersecurity trends for small businesses
- ❑ Report the Attack
- ❑ Communicate with Customers
- ❑ Learn from the Experience and document everything that plays out.

Thank you!

Please feel free to reach out for additional questions or help:

- joel@arbuckle.media
- arbuckle.media/book

STAY CONNECTED WITH TNS

- 🌐 Contact Business Development: TNSBusiness@novascotia.ca
- 🌐 Corporate website: <https://tourismns.ca/>
- 🌐 Consumer website: <https://novascotia.com>
- 🌐 inTouch Newsletter: <https://tourismns.ca/intouch>
- 🌐 Corporate Twitter: <https://twitter.com/TourismNS>
- 🌐 Corporate LinkedIn:
<https://www.linkedin.com/company/tourismnovascotia/>