Threatucation

End-User Security Awareness Training

The Business of Cyber Crime and Why Small Businesses Are Profitable Targets

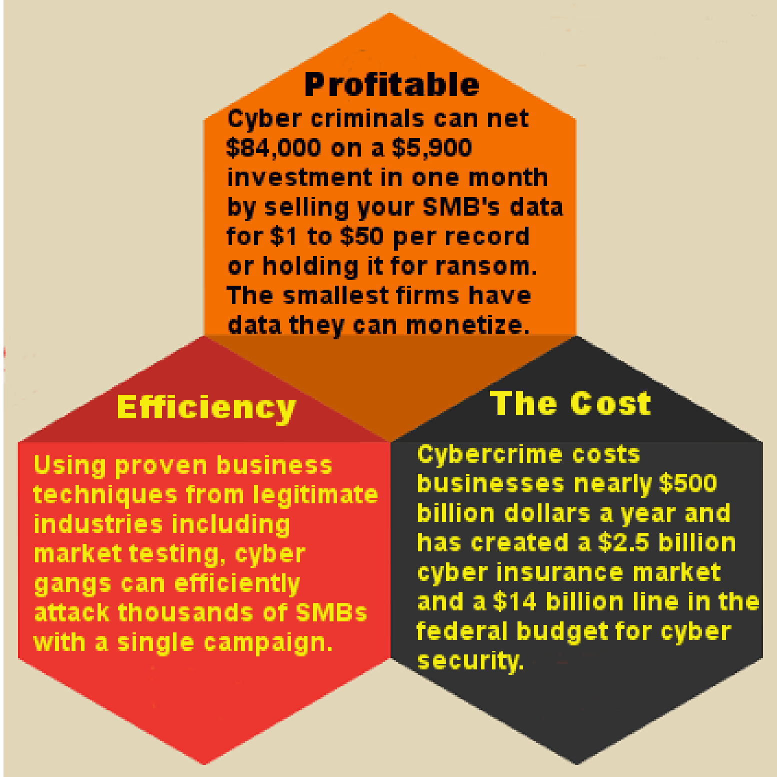
Cyber Criminals take their "businesses" as seriously as legitimate business owners by investing in more efficient methods of stealing data from all organizations

no business is too small

A report from **Threatucation**, Saturday, April 20, 2019
12 Osprey Ln., Ocean View, DE 19970 ~ 302-537-4198
info@threatucation.com ~ www.threatucation.com

Cyber Crime – A Lucrative “Business Model” at 1,400% ROI

Stereotypes of teens in basements vandalizing networks for the fun of it or of highly skilled hackers that concern themselves with only cracking large businesses and governments don't accurately represent the bulk of today's cyber crime organizations.



Profitable

Cyber criminals can net $84,000 on a $5,900 investment in one month by selling your SMB's data for $1 to $50 per record or holding it for ransom. The smallest firms have data they can monetize.

Efficiency

Using proven business techniques from legitimate industries including market testing, cyber gangs can efficiently attack thousands of SMBs with a single campaign.

The Cost

Cybercrime costs businesses nearly $500 billion dollars a year and has created a $2.5 billion cyber insurance market and a $14 billion line in the federal budget for cyber security.

Those teens have grown into cyber criminals and have joined common thieves who take their "businesses" as seriously as legitimate business owners by investing in more efficient methods of holding data hostage or stealing data that can be resold on underground markets.

Businesses of all sizes, down to mom and pop shops, have data hackers want.

These are the adversaries small business owners face today. The fact is, your small business is attacked multiple times a day via phishing spam or more targeted attacks if your data’s value warrants it.

The cyber security firm Trustwave reports **a cyber criminal can net $84,000 on a $5,900 investment in 30 DAYS** stealing and reselling data, such as seemingly harmless contact info for executives, employees, customers and vendors.

The data you store on yourself, your customers, your employees and vendors can fetch anywhere from 50 cents per record on the Dark Web (aka Deep Web) underworld for basic contact info to thousands of dollars for login credentials for online financial accounts.

As long as that kind of ROI and profit remain viable, and the risk of getting caught remains low, cyber criminals will invest in more innovative and efficient ways to steal your data and / or your money.

And they have no conscience about it. Their lack of conscience is so deep-rooted that they actually advertise their “honesty” to fellow thieves and rate the trustworthiness of each other’s services in feedback systems a la eBay.

Perhaps ironically, they take their own security and privacy more seriously than many small business owners by going to great lengths to protect their anonymity on the web to avoid suspicion and detection.

To combat these cyber criminals, you must make your business less profitable to them. To do that, you need to make your business less vulnerable.

Cyber Criminals – What's Yours, Is Theirs

How Many of These Data Types does your SMB Store?
What Hackers Want
* Account Login Credentials
* Personally Identifiable Information
* Credit Card Info
* Medical Records
* Any data that can be used to fraudulently apply for loans, credit cards, drugs, etc.
$

Cyber criminals approach their "businesses" with a mindset that they have a "right" to your data without compensating you for it. They profit off of your hard work by stealing and reselling your data.

They resell your data on the Dark Web, a vast online marketplace for engaging in not only stolen data but also illegal gun and drug sales and even hiring an assassin (yes, really).

As a business, we are mostly concerned with the resale of stolen data and services and tools used in cyber crimes. That data can be anything from contact records to account login credentials.

As data is stolen, it is re-sold and/or matched against existing data and combined into comprehensive personal dossiers on individuals or organizations that can be sold to cyber criminals to create new identities to commit various types of fraud, including bank, credit, insurance and medical frauds.

Consider this ad on the Dark Web from a cyber criminal named "OsamaBinFraudin".

"hello this ad is for usa profiles that have been freshly created and already currently have 720 credit scores or higher with no current bad history and no fraud alert you can use profiles for your own identity to get loans cars housing anything u can use a identity with perfect credit the profile will come with full name addresses associated with profile ssn dob credit karma login to verify credit score price is high because these profiles are pre built and already have high credit scores and you can use these identities as your own long as you like."

The advertised profile was offered for $454.05. How many of your customers have similar credit ratings? How well do you protect the data you store about them?

Data can also be encrypted and held hostage until a ransom from a few hundred to thousands of dollars is paid. If you pay the ransom, you may not get any of your files, or only a subset, until you pay more money. You then become marked as a patsy for future ransom demands.

Ransomware has become extremely popular for cyber criminals. The Check Point Threat Intelligence Research Team found the Cerber Ransomware organization infected 150,000 users in 201 countries with the author raking in $78,000 in July 2016 and $946,000 annually -- just from its affiliate operations.

This chart **shows the value of data, from all sizes of businesses, on the dark web**

RECENT PRICES FOR GOODS ON THE DARK WEB	PRICES
Credit Card Numbers and Associated Data	$7 each
Basic Contact Information	$.50 - $1.00
Full Identities (Name, Birth Date, SSN, Account Numbers, etc.)	$15 - $65
New Identity Package (Driver's License, SSN, utility bills)	$90
Popular Online Business Payment Account Login Credentials	$20 - $149
Popular Online Payment Account Login Credentials (Based on account balance)	$80 - $600
Bank Account Login Credentials (based on account balance)	$40 - $500
U.S. Airlines Points Accounts (based on amount of points)	$60 - $450
Medical Records	$50 - $60
RECENT PRICES FOR SERVICES ON THE DARK WEB	**PRICES**
Hacking Popular Email Accounts (Gmail, Yahoo, AOL, etc.)	$129
Hacking Social Media Accounts (Facebook, etc.)	$129
Hacking Corporate Email Accounts	$500
Scans of Counterfeit Driver's Licenses	$14 - $20
Ransomware (what ransom authors make from victims)	$300 - $28,000+
Transfer Funds from Online Accounts to Buyer's Account (Based on the account balance)	$225 - $950
Crypters (for Ransomware attacks)	$80 - $440
Exploit Kits	$100 - $135
Hacking Tutorials	$20 - $40

*Source: Dell SecureNow

As the table shows, the prices commanded on the Dark Web create lucrative opportunities for criminals and the prices to commit the crimes present a low barrier to entry.

Cyber Gangs – Increasingly Efficient, Sophisticated

As a small business that relies solely on traditional security solutions, you represent not only easier prey because you don't have the resources for industrial-strength security like large enterprises but you also offer an easier conduit to break into larger companies such as vendors or customers.

The infamous Target attack started when an employee at a Target HVAC vendor opened an infected email that contained malware that gave the hackers the access needed to steal the company's Target vendor login credentials. Before long, 40 million credit cards had been stolen.

Every small business, including mom and pop shops, stores sensitive data behind low security barriers and is a potential victim of Ransomware demands. The market is seemingly endless for hackers.

Hackers don't need to be particularly skilled, either. They can outsource their attacks to third parties or rent the tools necessary much like you do in your business. Using cheap email to distribute their malware and scams, they can easily attack thousands of small businesses at a time.

To more efficiently accomplish their tasks, "businesses" in the sophisticated Dark Web underground are highly organized and operate just like legitimate businesses:

Look Familiar? Legitimate vs. Cybercrime Business Models

Business Types & Models	**Legitimate**	**Cybercrime**
Startups to Mature Businesses	Y	Y
Specialists, Niche, Brokers, Joint Ventures	Y	Y
Sub-contractors	Y	Y
Franchise and Affiliate offerings	Y	Y
Guarantors to facilitate transactions	Y	Y
Products and Services	**Legitimate**	**Cybercrime**
Commoditized	Y	Y
Specialty	Y	Y
Outsourced	Y	Y
Marketing	**Legitimate**	**Cybercrime**
Vertical and Horizontal Markets	Y	Y
Unique Selling Propositions	Y	Y
Pre-launch Market Tests	Y	Y
Demo Versions	Y	Y
Promotions and Discounts	Y	Y
Testimonials and	Y	Y
Customer Service	**Legitimate**	**Cybercrime**
Technical support including 24x7	Y	Y
Product updates	Y	Y
Guarantees on products and services	Y	Y
Return on Investment	**10% - 25%**	**Up to 1,425%**

As a study by UBM in 2016 found, "Businesses aren't up against hordes of elite hackers but an industry efficient at finding those who are vulnerable." And hackers have concluded that **small businesses are the most vulnerable**.

Seemingly random spam attacks that your small business is subjected to every day in your email inboxes are actually part of an automated marketing campaign that has been A/B tested for its effectiveness.

Packed with infected links and file attachments, those emails are intended to steal login credentials the hacker can use to bypass your traditional security solutions, or install Ransomware on your systems.

That same UBM study stated that "**The most common weak spots are employees who get caught by attacks that use social engineering**, and under-budgeted IT teams that don't have the necessary skills, tools, or time to properly patch and defend complex, sprawling networks."

Don't think you have a complex, sprawling network? Compared to much larger organizations you don't, but consider that every single piece of hardware, software, employee, customer and vendor you have presents a potential vulnerability – one of dozens in even the smallest systems.

You can do your part to make cyber criminals' "businesses" less profitable by:

- Using security products that go beyond traditional signature- and definition-based solutions
- Offering your end-users security awareness training that teaches them how to:
    - Avoid bad practices that lead to data breaches
    - Recognize common social engineering scams
    - React properly to those scams
- Keeping your security solutions updated
- Keeping your applications and hardware updated
- Keeping your end-users updated on the latest threats
- Monitoring your network for suspicious activity before damage is done
- Frequent, random testing of your end-users' susceptibility to threats
- Adjusting security measures as needed based on test results

You can also join our End-User IT Security Group on LinkedIn via the link found at http://www.enduseritsecurity.com.

Sincerely,
Eric Magill
Owner, Threatucation
302-537-4198
https://threatucation.com
ericm@threatucation.com

Threatucation

End-User Security Awareness Training

The Threatucation End-UserIT Security Program

Call 302-537-4198 to Join

The **Threatucation End-User IT Security Program** protects against attacks on your last line of defense – your employees – by creating a culture of security that:

- **Develops or updates an Acceptable Use Policy** to govern use of network resources in the office and on the road
- **Presents the AUP to your staff** to show how it protects the company and the real-life consequences of violations
- Shows your employees **how to respond if they are victimized**
- Enables you to confidently implement new technology (i.e., mobility, BYOD) without delay over security concerns
- **Assures your customers and vendors** you take their data seriously, too
- Maintains your employees’ diligence with alerts on the latest scams
- Measures the training’s effectiveness and follows up with ongoing training
- **Enforces your acceptable use policy** with security that follows your employees wherever they access your data

Call 302-537-4198 to get started!