BUSINESS IDENTITY THEFT
WHAT YOU SHOULD KNOW

💡 Webinar will begin promptly at 2pm ET. All speakers will remain muted until that time.

💡 This webinar is being recorded and will be shared with all registrants.

HOSTED BY:

SIGNATURE SPONSOR

TREND MICRO™
education

AFFILIATE SPONSOR

IDENTITY PROTECTION SERVICES
✓ **Convening** partners who recognize strength in the security collective

✓ **Educating** individuals & organizations on cybersecurity best practices

✓ **Amplifying** collective efforts to increase cybersecurity awareness

[www.staysafeonline.org](http://www.staysafeonline.org)  
[@staysafeonline](https://twitter.com/staysafeonline)
Thanks to our National Sponsors

Over 10,000 webinar attendees

Over 5,000 workshop attendees

Over 15,000 subscribers

Signature Sponsor

TREND MICRO

education

Affiliate Sponsor

GENERALI

GLOBAL ASSISTANCE

IDENTITY PROTECTION SERVICES

Strategic Partner

ITSP MAGAZINE
Today’s Guest Speaker

Brittani Johnson
Marketing Manager,
Identity & Cyber Protection Services

@GeneraliGA_NA
IrisIdentityProtection.com
BUSINESS IDENTITY THEFT

WHAT YOU SHOULD KNOW

Presented by Brittani Johnson, Marketing Manager
BUSINESS IDENTITY THEFT DEFINED

According to the National Cybersecurity Society, business identity theft is defined as a type of identity theft committed with the intent to defraud or hurt a business by creating, using, or attempting to use a business’ identifying information without authority.
CYBER EDUCATION IS CRITICAL

28% of cyberattacks target small businesses.

66% of small businesses had at least one cyber incident in the past two years.

$2.74 MILLION
The average data breach cost for organizations with less than 500 employees.

27% Ransomware now accounts for 27% of malware incidents.
WHY SMBs ARE A TARGET

• Larger bank account balances
• Ease in opening new accounts
• Higher credit limits
• Invoicing and payment terms
• Minimal security
• Easy access to business information
A FEW EXAMPLES THROUGH THE YEARS

In Georgia, criminals purchased a cell phone & registered it under the name of “Georgia Powers” to divulge their credit card data.

A Lithuanian man pleaded guilty to stealing $100 million from Google and Facebook via forged invoices, contracts, etc.

A phishing scheme targeting the CFO of a small manufacturing company resulted in over $120,000 in stolen company funds.
ACCESS TO COMPANY EIN / DUNS NUMBERS

- Easy access to company info via
  - Company’s payroll or accounting department(s).
  - Company’s business credit report provided by a credit bureau, including Dun & Bradstreet.
  - Hired services to research a company’s EIN.
- Publicly available records of local or federal registration forms.
- Unreliable or not trustworthy companies/brokers.
THE IMPACT OF BUSINESS IDENTITY THEFT

TAX/CREDIT CARD FRAUD

• Access to EIN and publicly available information are, in most cases, enough to file fraudulent returns & apply for business credit cards.

• Phishing scams and business email compromise (BEC) attacks

• In 2019, the FBI’s Internet Crime Complaint Center (IC3) received 23,775 BEC complaints with adjusted losses of over $1.7 billion.

FRAUDULENT LOANS

• Easy access to private funds that may not always require high levels of verification.

• Online applications

• Disgruntled and/or negligent employees
HOW TO MITIGATE RISK

• Determine **who needs your EIN/DUNS numbers**
• **Regularly monitor** your business credit reports
• **Screen companies** before conducting any business
• **Use antivirus software & keep it updated**
• **Secure** your networks
• **Use strong passwords** & multifactor authentication
• **Make cybersecurity part of your company culture**
• **Maintain an up-to-date cybersecurity response plan**
• **Provide ongoing training** to all employees on security info management & cybersecurity threats (i.e. ransomware, malware, phishing, etc.)
• **Monitor & control physical access**
• **Consider a comprehensive identity protection service**
VICTIM OF BUSINESS IDENTITY THEFT?

- Always start with a police report
- File a complaint with the FTC at IdentityTheft.gov
- Report the theft to your financial institution and any other financial institutions involved
- Report the theft to the IRS and your local state administration
- Place a fraud alert on business credit report by contacting the four credit reporting companies:
  - Dun & Bradstreet
  - Equifax
  - Experian
  - TransUnion
- File a complaint with the FBI’s Internet Crime Complaint Center (IC3) if victim of BEC, ransomware, or cyber attack
THANK YOU!

FOR MORE INFORMATION, VISIT IRISIDENTITYPROTECTION.COM
OCTOBER MEANS...

1. HALLOWEEN
2. PUMPKIN SPICE LATTES
3. CYBERSECURITY AWARENESS MONTH

STAYSAFEONLINE.ORG/CYBERSECURITY-AWARENESS-MONTH
Become a Cybersecurity Awareness Month Champion:
https://staysafeonline.org/cybersecurity-awareness-month/champions/
Upcoming Webinars

• **July 22**: How to Get Involved in Cybersecurity Awareness Month

• **July 30**: Cybersecurity Q&A Part 2

• **August 11**: Cyber Essentials with CISA

• **August 27**: Cybersecurity Q&A Part 3

All of our events are located here: https://staysafeonline.org/events/