CyberSECURE

Prevention | Mitigation | Response

AN EMERGENT THREAT. A TARGETED COMMUNITY. AN INNOVATIVE EFFORT.

OVERVIEW

Cyber security poses a unique threat to the Jewish community. As technology becomes more integrated, the Internet of Things more expansive, and as organizations become more reliant on cyber systems, both individuals and institutions have increased exposure to potential cyberattacks. These attacks can cause reputational, financial and operational harm.

The Secure Community Network's **CyberSECURE** program represents the first comprehensive cyber security effort for any faith-based group in North America. In partnership with the United States Department of Homeland Security and key private sector partners and other stakeholders, SCN is innovating an effort to address the unique cyber security concerns of the Jewish community in a comprehensive, cost-efficient and operationally effective manner.

Through expertise and partnership, the **CyberSECURE** initiative will minimize our communities' vulnerabilities while protecting our data, networks, programs and members.

CYBER THREAT BY THE NUMBERS

200

Average organization uses 200 applications, from remote devices to cloud services

$1,000,000,000

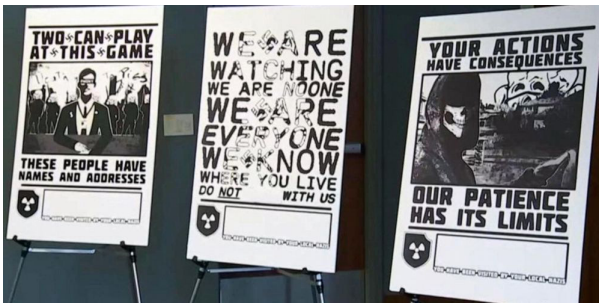
Ransomware: a $1 billion a year industry and growing

300,000

Increased number and severity of attacks, such as WannaCry, which impacted more than 300,000 people in over 150 countries

CURRENT THREATS TO THE COMMUNITY

Communities have been targeted by generic cyber attacks as well as non-state actors, including white supremacist groups:



- Prosecutors in Seattle announce charges against four alleged members of the neo-Nazi group Atomwaffen Division for cyber-stalking and mailing threatening communications to journalists, including Swastika-laden posters stating, "You have been visited by your local Nazis." https://www.heraldnet.com/news/former-arlington-man-and-4-others-arrested-in-neo-nazi-case/
- Cyber-criminals have launched a fake coronavirus threat map website to steal personal information from a panicked public. https://www.infosecurity-magazine.com/news/infostealing-coronavirus-threat/

BENEFITS

The **CyberSECURE** initiative is designed to increase Jewish organizations' cyber hygiene and security posture, arming participating organizations with the ability to more easily recognize, prevent, and respond to cyber threats:

Awareness: participating organizations will receive alerts of active or potential cyber threats targeting or affecting the Jewish community, as well as best practices and security considerations.

Education: participating agencies will be invited to attend informational webinars and trainings on relevant topics, including cyber threats and prevention, protection, mitigation, response and recovery.

Best Practice: initiative members will have access to a resource library of guides and materials that provides individuals and organizations with cyber security information on hand for easy reference.

Solutions: working with public, private and non-profit partners, participating organizations will have exclusive access to solution-sets available through the initiative.

CYBER SECURITY STATISTICS

$6 TRILLION
The expected cost of cyber crime damage annually by 2021 (up from $3 trillion in 2015)

$11 BILLION
The expected cost of global ransomware in 2019. An organization will fall victim to a ransomware attack every 14 seconds

43% CYBER ATTACKS
The percentage of cyber attacks aimed at small organizations.

197 DAYS
The number of days for an organization to detect a breach in their network.

81% DATA BREACH
The percentage of data breach victims that do not have systems in place to self-detect data breaches.

Source:
www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics.html | www.thebestvpn.com/cyber-security-statistics-2018

DHS PARTNERSHIP: FEDERAL RESOURCES, LOCAL IMPACT.

As the official homeland security initiative of the Jewish community in North America, SCN's partnership with the United States Department of Homeland Security (DHS) enables efficient information exchange with the federal government – leveraging federal expertise, empowering organizations with critical information and services, and ensuring that vulnerabilities and threats facing the Jewish community are properly addressed. The DHS and SCN partnership includes:

- Incident reporting relationship directly with top DHS analysts
- Access to DHS network monitoring capabilities
- Analytical products with cyber threat information and analysis
- Training and coordination with DHS cyber experts
- Input on best practices

SCN actively engages our federal partners to operate at the intersection of our communities and federal law enforcement in order to apply unique analytic perspectives and ensure shared situational awareness. Our partnership enhances our ability to prepare for, prevent, and respond to cyber incidents targeting Jewish communities across North America.

As a participant in the CyberSECURE initiative, organizations have unique access to a special reporting relationship. When an issue is observed or concern is raised:

1. Follow internal reporting protocols;
2. Report the Incident to the SCN Duty Desk;
3. SCN will work with your organization and our federal partners, including the FBI and DHS, to appropriately report the incident.

To report a cybersecurity threat or incident, please contact:
SCN Duty Desk at 844.SCN.DESK
or email DutyDesk@SecureCommunityNetwork.org