SOCIAL MEDIA AWARENESS

Social media is increasingly being used to obtain personal information and commit cybercrimes, posing a threat to individuals and organizations. The best way to prevent attacks is to practice smart social media habits and monitor posts.

CONSIDER THIS...

97%

...of adults ages 16-64 say they logged onto at least one social network in the past month.

$780 BILLION

...in mobile payments on smartphones, tablets, and other portable devices by US citizens in 2017 alone.

936,000

...total comments, status updates and photos are posted to the Facebook platform every minute.

THE RISKS OF SHARING INFORMATION

VIRUSES

An attacker can potentially infect millions of computers with a virus embedded in a website or a third party application.

TOOLS

Attackers may use tools that allow them to take control of a user's account, potentially exposing private data and access to contacts.

SOCIAL ENGINEERING ATTACKS

Attackers may mask their activity behind what appears to be a trusted social networking service or user, yet the content contains a malicious link or request for personal information.

IDENTITY THEFT

Given even a few personal details from social networking sites, attackers may be able to assume your identity or the identity of one of your contacts.

"Socializing Securely: Using Social Networking Services,"
United States Computer Emergency Readiness Team (US-CERT)
Department of Homeland Security,
accessed 21 June 2018

SECURE COMMUNITY NETWORK

PROTECTING

YOURSELF ON SOCIAL MEDIA

THE INTERNET IS A PUBLIC RESOURCE

Be mindful that anyone can potentially see what you post – including text, pictures and videos. Once you post information online, you cannot retract it. While the information may be taken off the internet, a version of it may still exist on other user's devices.

BE AWARE OF STRANGERS

People are able to easily shield their real identity behind a computer screen. Limit the people that you connect with online to those that you know. If you interact with someone that you do not know, be cautious of how much information you reveal or of agreeing to meet in person.

KEEP SOFTWARE UP TO DATE

Make sure that software, particularly your web browser, is up to date so that attackers cannot take advantage of problems or vulnerabilities. If offered, enable automatic updates.

USE AND MAINTAIN ANTI-VIRUS SOFTWARE

Anti-virus software protects your computer against any potential or known viruses, so you can catch the virus before it does any damage.

'REAL-TIME' POSTING EXPOSES VULNERABILITIES

Avoid posting pictures online in real time when you are away from home, as it exposes potential vulnerabilities.

SEPARATE YOUR CONTACTS FROM YOUR APPLICATIONS

Do not allow applications to access your contacts. This can create conditions that spawn future phishing emails from a perpetrator leveraging your email account and contacts.

USE STRONG PASSWORDS

Protect your accounts by using strong passwords that are not easy to guess. Avoid using the same password for multiple accounts, and change them regularly. If your password is compromised, someone else can access your account, pretend to be you, obtain your personal information, steal information about a company you work for, etc.

LIMIT THE AMOUNT OF PERSONAL INFORMATION YOU POST

Do not post anything that can make you vulnerable to others on the internet. Avoid posting information about your routine or your address, and if someone posts information about you, make sure that you are comfortable with the information shared.

AVOID STORING BANK AND FINANCE INFORMATION ONLINE

Do not save banking information on any social media platforms. Providing such information enables attackers to hack financial accounts and commit theft.

PRIVACY SETTINGS

Take the time to review the privacy settings on all your applications and ensure you are comfortable with the information being collected on your account and how it is being used.

LOG OUT

Remember to always log out of a social media account after using it, especially when using a public computer. Having a continuously logged in account makes you vulnerable to attackers.

"Staying Safe on Social Networking Sites,"
United States Computer Emergency Readiness Team (US-CERT)
Department of Homeland Security,
accessed 20 June 2018

The Secure Community Network (SCN), a non-profit 501(c)(3), is the official homeland security and safety organization of the Jewish community in North America. Established under the auspices of The Jewish Federations of North America and the Conference of Presidents of Major American Jewish Organizations, SCN is dedicated to ensuring the safety and security of the Jewish community through increased awareness, improved protection, enhanced preparedness, and effective response.

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