Social Media Cybersecurity Best Practices

www.staysafeonline.org

@staysafeonline
NATIONAL CYBER SECURITY ALLIANCE

www.staysafeonline.org

@staysafeonline
Over 6,000 webinar attendees

Over 2,000 workshop attendees

Over 15,000 subscribers

Signature Sponsor
TREND MICRO

Initiative for Education
DIGITAL SAFETY OUTREACH

Contributing Sponsor
INFOSEC

Strategic Partner
ITSP MAGAZINE

https://staysafeonline.org/cybersecure-business/
Social Media Best Practices

- “In the News”
- Trend Micro Threat Briefing
- Digital Audit
- Password Security
- Two Factor Authentication
- Limit Access
- Take care with what you share
- Secure Connections
- Privacy settings
House of Wolf Pub

• Small pub in England

• Disgruntled employee who had retained access to the Facebook and Twitter profiles hijacked the page and launched into a rant.

• The assault spread to the pub’s website where the hacker created a new page with a ransom request “This will remain on the HOW website until you pay me. Please uphold your agreement and pay up.”
Instagram Influencers—Influenced to submit credentials

- Instagram influencers are part of a multi-billion-dollar industry

- Criminals pose as a brand interested in sponsoring the targeted influencer “What is the cost of an advertising post on your page?”

- Each email included a convincing looking phishing link, which appeared to go to the sender’s real Instagram account. Instead, it directed the victim to a fake Instagram login page, which then sent the victim’s password to the hacker.

- With credentials, the criminal can hold the account for ransom.

“The hacker took everything from 24-year-old Californian Lindsie Comerford. Her email, online banking, and her Instagram account, which had more than 41,000 followers.”

Criminals gain access to your Pinterest account
- Will pin topic that gets repeatedly shared
- Report and delete unauthorized pins
- Update credentials
In 2017, a group called OurMine appeared to take control of the main HBO accounts, as well as those for the network's shows including Game of Thrones.
Social Media and Cybercrime

Brook Stein
Startling Facts about Cybercrime

• 1 in 5 organizations worldwide infected by malware distributed by social media
• Social media cybercrime increased 300 fold from 2015-17 according to FBI report
• In 2018, RSA fraud analysts reported a 43% increase in social media attacks compared to an increase of only 12% of phishing attacks.

Why Social Media?

• Billions of users access social media daily
• Social media makes it easy to share and pass on just about anything – including malware
• Researchers found that social media platforms, on average, have 20% more methods to scam and rip off consumers than other websites, including advertisement, share buttons and plug-ins
• Plus, most users have hundreds, if not thousands of connections on social media platforms making them ideal to spread malware with few negative consequences

How cybercriminals use social media

• Used widely to spread malware – malicious links, malicious advertising
• Sales of tools of social media – lines between social media and dark web are becoming blurred
• Leveraging hacked credentials to refine malware and scam targeting
• Leverage oversharing to compromise or target online accounts
Staying Safe on Social Media

• Think before you click or post
• Be careful of "oversharing" and never share personally identifiable info on social media (DOB, SSN, phone number, e-mail, etc.)
• If asked for DOB, consider using a nonsense date such as 1/1/1904
• Never use a work email address on social media. If you must, create a separate account.
Social Media Best Practices

- Digital Audit
- Password Security
- Two Factor Authentication
- Limit Access
- Take care with what you share
- Secure Connections
- Privacy settings
Digital Audit

- What accounts do we have registered? Include apps.
- Who has access to them?
- What information (photos, videos, etc.) have been posted to these accounts?
- Do we have social media policies and procedures? What are they? Do they need updated?
Password Security

--Example: 
ILikeToEatIceCreamOnSunday$

• **Length trumps complexity**
• Use unique passphrases
• Discourage password sharing among colleagues
• Select security questions only you know the answer to
• Change passphrases quickly if there is a breach
• Use password managers
Authentication

- Enable 2FA or Multifactor Authentication on all accounts.

- **Something you know** (like a password or PIN), **Something you have** (like a smart card), or **Something you are** (like your fingerprint).

- Microsoft: Your account is more than 99.9% less likely to be compromised if you use MFA.
Limit Access

- Principle of Least Privilege
- On-boarding & off-boarding considerations
- Physical security considerations
Take Care with What You Share

• What you post could have a bigger "audience" than you think.
• Once posted, always posted
• Get someone's okay before you share photos or videos they're in.
• Discourage office photography
• Keep personal info personal
• Not everyone is your friend

“It’s this new app—you put in your social security number, and it makes you look like a cat.”
Secure Connections

- Just say no to public wifi
- Disable Auto-Connect
- Virtual Private Networks
Privacy Settings

- Configure immediately when signing up for a new platform
- Do annual privacy setting checkup
- Experian resource: How to configure your privacy settings: https://www.experian.com/blogs/ask-experian/how-to-manage-your-privacy-settings-on-social-media/
- NCSA’s Privacy Settings Resources: https://staysafeonline.org/stay-safe-online/managing-your-privacy/manage-privacy-settings/
Your Social Media Privacy Settings Matter

• Never give more information than is necessary to operate an online account. Usually this includes an e-mail, username, and a password. If your birthdate is required, consider using a nonsense date like January 1, 1904 since your real birthday is tied to important IDs, like your driver’s license, social security number, or passport.

• Never use a work email address and consider creating a separate one for social media sites. Make sure that your posts are not indexed into search engines. Each social media site handles this in a different way.

• Be cautious of what you post on any social media site. Just because you can post it, doesn’t mean that you should.

Source: Rick Ferguson, Trend Micro, Inc
http://blog.trendmicro.com/your-social-media-privacy-settings-matter/
NEW YEAR’S RESOLUTION?
STOP HITTING “PAWS” ON THAT SYSTEM UPDATE.

#UPDATEMEOW

Disclaimer: No component or product can be absolutely secure.
Social Media Cybersecurity Best Practices

www.staysafeonline.org

@staysafeonline

@danieleliot