SMALL BUSINESS.

BIG IDEAS.

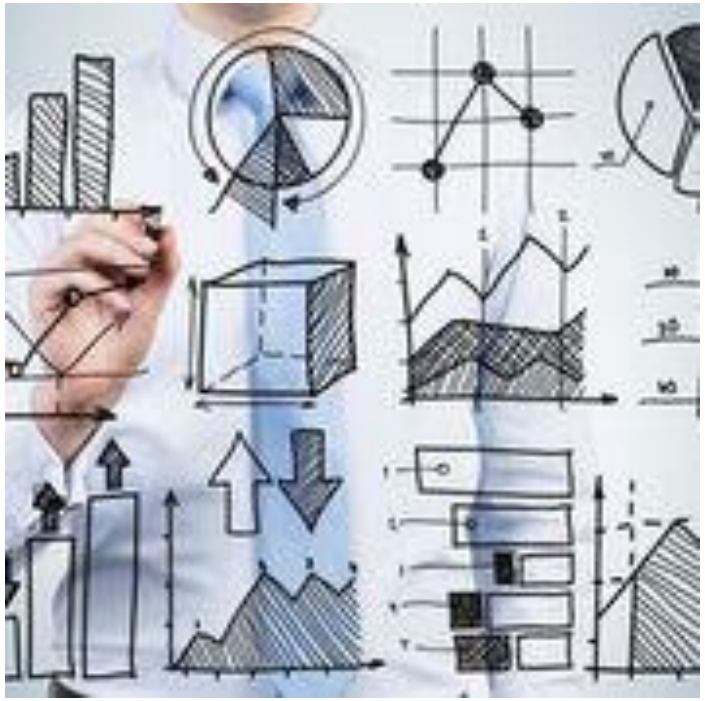
RIM TECHNOLOGIES

Sara Kinney
www.rimtech.co
719.332.0423
@rimtechco
@saraekinney

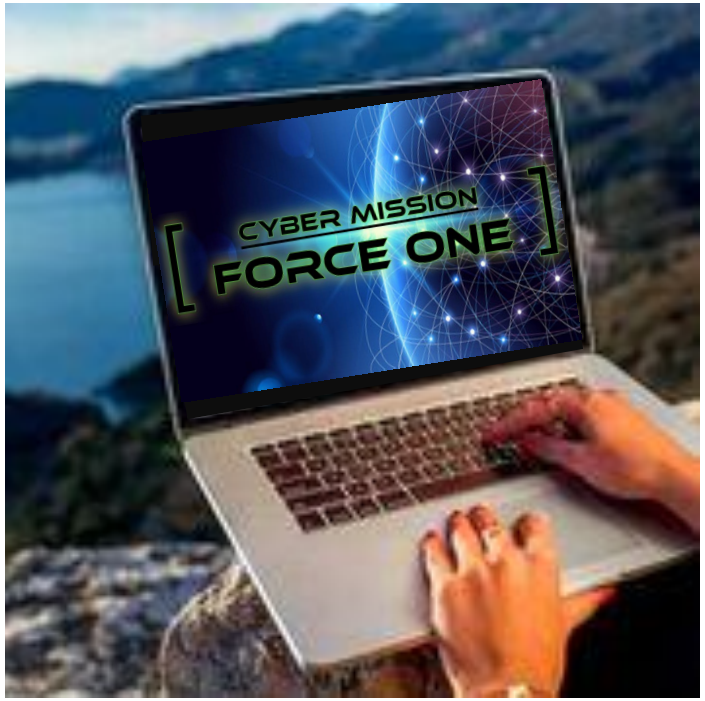
RIM TECHNOLOGIES

#imagine

#create



#build



www.rimtech.co

Readiness: Phase 1

Cyber-vandalism occurs when an outside party, regardless of identity or motive, takes control of an online communication channel and misdirects it.

Business owners should plan and train prior to an incident, and prepare approved processes and material for the recovery and response to cyber-vandalism.

1. Identify a social media stakeholder team to prevent and respond to cyber-vandalism

A direct chain of responsible managers should be aware of their role in the potential response to any social media cyber-vandalism, including the necessity of quick, decisive action. This team should be connected by email, phone, text and any other appropriate means of communication. The team should include, but is not limited to:

- Social media team
- Program manager
- Public Relations
- IT Security
- Senior leader/manager
- HR

2. Review Individual App/Platform Resources

Online-based communication tools offer resources, each with unique strengths and limitations. Awareness of this support and their unique characteristics is beneficial before an incident:

- **Facebook:** Facebook Security Tips (link is external); Facebook Security Settings (link is external); Learn extra security features (link is external) including approvals, notifications, trusted contacts and mobile security
- **LinkedIn:** LinkedIn Safety Center (link is external); Prevention Tips (link is external); Password Guidelines (link is external); Frequently Asked Questions | Reporting Inappropriate Content, Messages, or Safety Concerns (link is external)
- **Instagram:** Instagram Privacy & Safety Center (link is external)
- **Twitter:** Safe tweeting: the basics (link is external)
- **Google:** Keeping your account secure (link is external)
- **Hootsuite:** Social Media Security
- **Evernote**

3. Establish Stakeholder Rapid Outreach Plan

- Prepare a list of internal and external contacts and processes for a cyber-vandalism incident:
- Who is the point of contact for the app or platform when an incident occurs (see Phase 2: Recovery for list)?
- Who is on your social media team?
- Who are your key communities and audiences on social media and other channels you must alert?
- Incorporate relevant contact information:
- Emails; Phone Numbers; Social Media Handles; Hashtags; Listservs and more.

4. Create Communication Templates

- Pre-populate different types of messages.
- Emails; Texts; Social media posts and more.
- Communicate essential information to convey the nature of the compromise, for example:
- An account is compromised; An administrator cannot access an account; A username and/or password for an account is compromised; Information on the account is unauthorized.

5. Review Secure Social Media Best Practices Checklist

- Institutionalize secure web standards, such as HTTPS, as a foundation for secure social media:
- Using an URI scheme, such as HTTPS, establishes a fast, private, and secure connection due to its strong encryption benefits
- Create a social media policy for cyber-security.
- Train stakeholders and others on the procedures and policies of social media cyber-security.
- Follow best practices for secure passwords.

6. Evaluate Two-Step Verification

This type of authentication verifies a user attempting to access a device or system. It requires confirmation of two consecutive, yet dependent, entries. It may not be applicable to those without mobile devices or in secure environments prohibited entry of such items. It may also require the use of third-party management tools to effectively allow multiple content coordinators.

- **Facebook:** Facebook's Login Approvals (link is external); ZDnet.com supplemental step-by-step guide (link is external).
- **Google and YouTube:** Google 2-Step Verification (link is external).
- **LinkedIn:** LinkedIn's Two Step Verification (link is external).
- **Twitter:** Twitter's Two Step Verification Process (link is external).

7. Review Special Guidance Per Common User Responsibility

- **For Supervisors and Directors:** Confirm policy is clear, accessible, and distributed among employees. Review, approve, and document all social media accounts regularly. Identify and eliminate rogue accounts. Instruct staff administering accounts to adhere to established policies.
- **For Social Media Managers:** Make security a part of regular social media meetings. Conduct security checks on a regular basis. Regularly update passwords. Keep the list of social media accounts updated. Keep account manager contact information accessible and updated. Remove access for users who are no longer with the agency. Develop a secure method of storing account names, owners, and passwords.
- **For Social Media Coordinators:** Use a protected device. Use protected connections. Do not post from an open Wifi network. Use a work VPN, 3G or the work-connected Internet connection. Generally, use network locations with strong firewalls and on standalone equipment. Preview shortened links to see the address of where they lead. Review the URL of a website in the address bar. Make sure the websites you visit use HTTPS encryption. If you are unsure of a link, double click the lock icon on your browser's status bar to display the digital certificate for a site.

Recovery: Phase 2

Alerts of suspicious activity on social media can come from anywhere, including social media itself. If the social media cyber-security stakeholder team or responsible manager determines an incident is in progress, remember that minutes and even seconds count. Within minutes you'll need to alert internal stakeholders, alert outside stakeholders to help you regain control, and act to isolate the compromise.

- Immediately: Alert your social media cyber-security stakeholder team, and CC them on following messages.
- Attempt to change passwords to isolate the incident (steps 2 and 3 ideally simultaneously with two employees)
- Contact the platform companies themselves to help regain control.

1. Contact Information to Recover Control After Cyber-Vandalism

- **Facebook:** Online form for Facebook (link is external)
- **Twitter:** Online form for Twitter (link is external)
- **LinkedIn:** Respond to and Report Various Issues (link is external)
- **Instagram:** Online form for Instagram (link is external)
- **Vine:** Online form for Vine (link is external)
- **Hootsuite:** Email: Support@hootsuite.com

2. Audit your social media inventory

- Audit your list of social media accounts, password holders, and hosted websites.
- Ensure no former employees, contractors or interns have access to current passwords.
- Review any third-party app you use to monitor or post to social media, such as IFTTT.
- Review your other digital services, including websites, for signs of cyber-vandalism and any vulnerabilities.

3. Confirm cyber-vandalism recovery process on different channels

- Once securing your other accounts, release messages alerting your communities that an incident is occurring and that steps are underway in order to recover cyber-vandalized accounts.

4. Initiate Restoration Activities After Regaining Account(s)

- Archive cyber-vandalism messages.
- Delete cyber-vandalism messages.
- Stop all pre-scheduled messages.
- Restore normal settings and features.

Response: Phase 3

Businesses must not only prepare for and recover social media accounts after a cyber-vandalism incident, they should also

quickly and effectively respond to their stakeholders and audiences as soon as possible using social media in order to maintain trust in digital services.

Initial responses to the cyber-security stakeholder team and the public should be within minutes of recovering control of your accounts.

1. Confirm Incident and Recovery

- **Cyber-security team confirmation:** Send initial report of recovery to social media cyber-security stakeholder team.
- **Public confirmation:** Distribute as soon as possible social media posts confirming the cyber-vandalism incident and your recovery of affected accounts. Announce a return to regularly scheduled activities.
- **Community confirmation:** Deliver additional communication with pre-determined internal audiences and stakeholders to prevent the spread of rumors and misinformation.

2. Confirm and Verify Changes to Access

- Review account holders.
- Confirm verification of login status.
- Confirm changes and updates of passwords.

3. Conduct a review of lessons learned

- What type of response worked well?
- Why did this work so well?
- What did not work?
- What unforeseen events occurred?
- What changes will lead to a better response?

4. Apply data and analysis of outcomes to improving your program

- Develop after-action report.
- Ensure future relevance with accurate information.
- Include lessons learned and best practices.

SMALL BUSINESS.

BIG IDEAS.

Sara Kinney
www.rimtech.co
719.332.0423
@rimtechco
@saraekinney