proofpoint.

BEST PRACTICES & TOP TIPS FOR AVOIDING / ADDRESSING SOCIAL MEDIA HACKS

THE BEST WAY TO ADDRESS A SOCIAL MEDIA HACK ATTACK IS TO AVOID IT IN THE FIRST PLACE

In the age of social media and as many companies are deploying employee advocacy programs—encouraging their employees to use their own social media networks to be brand advocates—organizations' digital risk footprint have been greatly expanded.

HERE ARE SOME BEST PRACTICES TO GUARD AGAINST SOCIAL MEDIA HACKS

- ☑ Make sure that your employee social media policy includes instructions about how to secure both branded and employee accounts.
- ☑ Partner with a vendor that can protect these accounts and alert you to potential packs proactively.
- ☑ Always be monitoring. And make sure that everyone who is responsible for monitoring social media is aware of the plans and workflow in the case of an attack.
- ☑ Make social media training for employees a priority, as well as part of the new employee onboarding process. Make sure to include instruction on how social media hacks like email phishing attacks happen, password best practices, etc. to best protect social media accounts. Try gamifying training to make it more appealing and encourage employees to complete the sessions.

IF A SOCIAL MEDIA HACK DOES HAPPEN, MAKE SURE YOU'RE PREPARED

- ☑ Have a clearly defined plan, specified roles and workflows in place—just as you would with a traditional crisis plan.
  - Make sure these are all clearly communicated to the key stakeholders across the organization.
  - Plans and workflows will differ depending upon whether a branded social media account or employee social media account was hacked.
- ☑ Partner effectively across your organization. Your scenario planning and resulting crisis plan and workflows should include the:
  - Social media team
  - Internal communications team
  - External communications team
  - PR / corporate affairs
  - Office of the CIO, CISO any other key information security and privacy management team members
  - HR management—especially in the case of an employee social media account hack
- ☑ As soon as an account is compromised, contact the proper authorities internally, as well as externally at both your social media management vendor and the social media platform to suspend the account, and delete any on authorized posts.
- ☑ Communicate with your stakeholders immediately. Even if you don't have details, you should let people know that you're aware of the incident, you're investigating, and you'll provide more information as soon as it's available. Deliver updates frequently, even if there's nothing new to report.
- ☑ Front-line employees are more credible spokespersons for the organization than CEOs or PR staff. Train the appropriate staff (from IT or credit card services, for example) and include them in the crisis plan.
- ☑ Practice to be prepared. Once your plan and workflows are in place, run some practice scenarios involving all parties. Incorporate any learnings into the process.

SAMPLE SOCIAL MEDIA HACK INCIDENT MANAGEMENT WORKFLOW / CHECKLIST TEMPLATE

If you believe that the social media channel you manage is being hacked, take the following steps immediately

- ☑ Contact information security:
  - [add specific name(s), emails, phone #s, including mobile phones and any IM info.]
- ☑ If your email has been phished, stop using TR email and switch to communicating via your personal account
- ☑ Contact the social media team to alert them to the situation
  - [add specific name(s), emails, phone #s, including mobile phones and any IM info.
- ☑ Change your passwords
  - At least 16 characters with special characters, upper/lower case, numbers
- ☑ File the customer support request with the affected social media channel
  - Twitter: https://support.twitter.com/forms/signin
  - Facebook: https://www.facebook.com/hacked?
  - LinkedIn: http://help.linkedin.com/app/safety/home
  - YouTube: http://productforums.google.com/forum/#!topic/youtube/FHx2yGzNF0o[1-25-false]
- ☑ Contact your representative at the affected social media channel(s) to escalate the support request
  - Twitter: [add specific name(s), emails, phone #s, including mobile phones]
  - Facebook: [add specific name(s), emails, phone #s, including mobile phones]
  - LinkedIn: [add specific name(s), emails, phone #s, including mobile phones]
  - [Add others as relevant]
- ☑ Instruct the representative or support team at the affected social network(s) to delete any unauthorized posts and temporarily disable the account until it is safely back under TR control

IF ACCOUNTS ARE HACKED AND UNAUTHORIZED CONTENT IS PUBLISHED

- ☑ Be transparent and honest—don't try to hide it
- ☑ Internally—use this as a teaching moment—an opportunity to remind key stakeholders and all employees about the importance of cyber security
- ☑ Externally—don't pretend it didn't happen. Issue a statement acknowledging what happened and apologizing for any offensive or confusing unauthorized posts. Review your social media marketing plans and suspend any posts that will be inappropriate in light of the hack.
- ☑ Make improvements to the process and then move on. Don't let it be a deterrent to your social media strategy.