Tools you can use:

ACCOUNT SECURITY TIPS

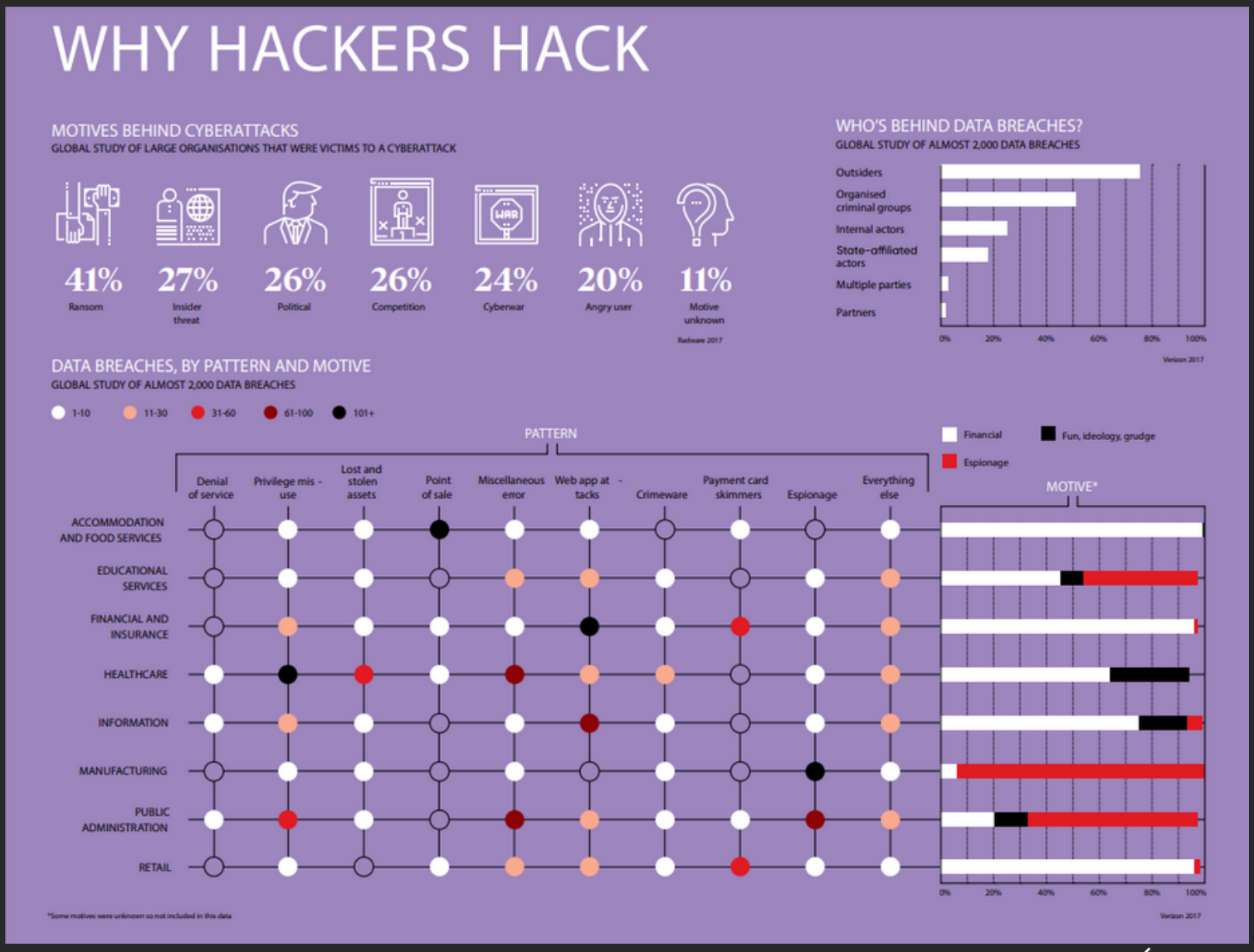
STEPS TO HELP PREVENT ACCOUNT HACKING

DENT
Model Magazine

ACCOUNT SECURITY TIPS

THERE'S A NEW HACKER ATTACK EVERY 39 SECONDS

Losing your social media account can be costly and time consuming. Social media accounts with a large following are prime targets for hacking. We've prepared this guide with some best practices to help secure your account against a breach.



DENT
Model Magazine

ACCOUNT SECURITY TIPS

WHY SOCIAL MEDIA IS THE NEW TARGET

As written by Sheera Frenkel from a New York Times article, “the human error that causes people to click on a link sent to them in an email is exponentially greater on social media sites… because people more likely consider themselves among friends.” By having a scam where people don’t expect it, they are less wary of a potential attack, so they don’t see the warning signs. Most people don’t see their profiles as valuable information goldmines. Hackers can use your contact list to reach new people, they can use your interests or habits to target email phishing scams, or even see your browsing or shopping history.

SOCIAL ACCOUNT HACKING IS BIG BUSINESS

Accounts with large audiences are a prime target because your account is valuable. There's 3 primary "styles" of hacking accounts:

1. Ransom Attacks: This is where a hacker will take control of your account and then offer to "sell" your access back to you - usually for an exceptionally high fee.
2. Business Hindrance Attacks: These usually are where a hacker will take control of your account and delete it robbing you of your followers, fan-base and the clout your account holds.
3. Humiliation: Hackers will take control of your account and post offensive/inappropriate/embarrassing content aimed at offending or driving off your audience or collabs.

Hackers either generate notoriety or income for successful account hacks

ACCOUNT SECURITY TIPS

WHY YOU SHOULD SECURE YOUR ACCOUNTS

First and foremost, it's time consuming to have your account stolen. Even if you're successful at re-gaining control of your account (without a ransom) it's still lost time not to mention stressful.
Second, it's expensive - time is money and if you end up being extorted for actual money; buying back account access is never cheap.
Third, it can cost you followers and partnerships. Starting over is a long road.

Creating unique and secure passwords is the best way to secure your accounts. We know it is a lot to keep track of, but if you want your social media and other accounts as secure as possible, use a different password for every account. That way, if one account is hacked, the others will remain secure.

SO EASY A KID CAN DO IT

No, really. There's websites, tutorials and apps for hacking social accounts. Anymore, if you have a phone and you can read you can get step-by-step instructions on how to breach someone's social media account.

ACCOUNT SECURITY TIPS

ACCOUNT SECURITY BEST PRACTICES

- Enable two-factor authentication on all social media channels.
- Never give account or page credentials to anyone who emails or direct messages you claiming to be customer support from the network itself.
- Never click too-good-to-be-true offers or dubious news articles, as these often lead to malicious apps or malware exploits.
- Never download any unsolicited apps, especially ones that have permissions to post on your behalf.
- Review the list of apps that have 3rd party access to your account. Remove any you don't recognize.
- Update your passwords and security settings regularly.
- Avoid password reuse at all costs.
- Be wary that your connections may be hijacked as a springboard to socially engineer other people profiles.
- Validate any odd or out-of-character requests through third party communications.

HAS MY INFO ALREADY BEEN LEAKED?

Check www.haveibeenpwned.com which has an easy search function to see if your email address has been leaked from some of the biggest hacks to date. While this site does not cover every leak, it should give you some insight into just how big of a risk cybersecurity is to our ever-connected society. If you do not show up on this site now, be wary that the next breach could have already happened, and you don’t even know about it yet. We suggest checking this site from time to time.

DENT
Model Magazine

ACCOUNT SECURITY TIPS

2 FACTOR AUTHENTICATION

Two-factor authentication adds an additional layer of security to the authentication process by making it harder for attackers to gain access to a person's devices or online accounts, because knowing the victim's password alone is not enough to pass the authentication check. Two-factor authentication has long been used to control access to sensitive systems and data, and online service providers are increasingly using 2FA to protect their users' credentials from being used by hackers who have stolen a password database or used phishing campaigns to obtain user passwords.

Instagram supports 2 Factor Authentication natively using Duo or Google Authenticator. You can set up 2FA by going to your Instagram app and opening the menu: Settings>Security> Two-Factor Authentication

Follow the steps outlined on screen to set up 2FA, generate your access keys and recovery codes.

NOTE: Your account recovery codes should be saved somewhere (NOT within your IG account). Screenshot them and save them on your phone, upload them to Dropbox or Google Drive or some other method of saving them. Should you ever need to recover your account you'll need these codes.

ACCOUNT SECURITY TIPS

PASSWORD BEST PRACTICES

The best protection against account theft is strong, complex passwords that are never reused between sites. This way, if one site experiences a data breach hackers don't end up with access to other accounts simply becuase the passwords are the same.

But, trying to create (and then remember) highly complex passwords over the myriad of online accounts you have isn't the most feasible process either. Fortunately, there's an app for that...

LastPass

LastPass is a password manager application that creates and stores complex passwords for all your accounts. It works on your computer and your mobile devices and best of all, it's free. You can even share your login information with other LastPass users without them needing to know your username and password information (and you can revoke it at anytime).

If you're interested in LastPass you can create an account here: www.lastpass.com

This is not a paid or sponsored advertisement. Jaze Companies/Dent receives no compensation if you decide to sign up for LastPass.

DENT
Model Magazine