NEED TO KNOW NEWSLETTER January 2021

Sharing isn’t always caring — especially online

Protect yourself by practicing OPSEC

OPSEC is a mindset

Social media has normalized sharing on the internet. But even the most innocent information, like photos from your trip, your weekend plans or job updates, should be thought of as oversharing in the age of social engineering. And that’s because every piece of information you share online can be used against you.

Staying secure gets more and more exhausting the more sophisticated cybercriminals become but practicing operational security (OPSEC for short) is a great way to frame your thinking when posting online. While the term is traditionally used in reference to military members or government officials, OPSEC in general is the practice of protecting yourself from enemies.

OPSEC checklist: 3 steps to staying secure

1. Limit personal information shared on your social profiles

While social media is all about chatting and sharing, you should be cautious about what you say and who can see it. Seemingly harmless information can give hackers the ammunition they need to launch a phishing attack.

In general, you should never share your location or plans, even though bragging about your upcoming vacation may be tempting. Hackers can use location data to tailor their attacks, while thieves may use it to case your place.

You should also avoid sharing details about your employer. And beware of photos and details that could give people answers to your security questions: things like which elementary school you attended, the street you grew up on and so on.

While having no social media at all is the best way to keep people out of your business, the next best thing you can do is keep a low profile.

2. Declutter your office — especially what’s in view of your webcam

You’ve probably heard the horror stories about hackers gaining access to webcams, but you might not have considered the ways in which you’re exposing yourself when you use yours.

In the era of virtual work, anyone can take a peek into your personal life on a conference call. That’s why you should be aware about what documents and other sensitive information are visible in your frame.

Before virtual meetings, clear your workspace, secure files and check reflective surfaces to get a glimpse at what others may be able to see. This will get you into the habit of ensuring personal materials are always out of sight.

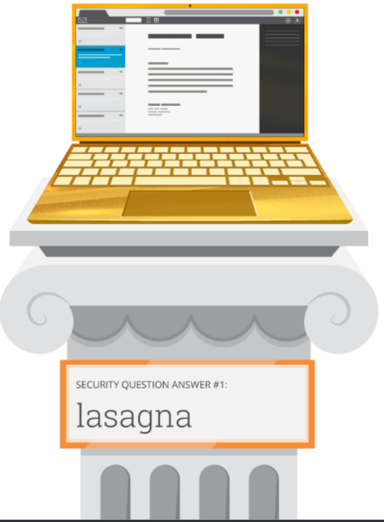
3. Get creative when setting up account security questions

When it comes to securing your accounts, your best defense is nonsense. Instead of giving standard answers to security answers, try responding with something silly or nonsensical. When asked what your childhood pet’s name was, for example, you might write “magenta” instead of “Buddy.” Or you may say you met your spouse at “lasagna.”

In addition to providing unique answers, you can also type them in all lowercase letters so they’re easy to remember.

Less is definitely more

When you create a new account, you’re likely used to providing an email address and password, but sometimes platforms ask for more. Whether it’s for marketing purposes or for “a personalized experience,” as they may frame it, doesn’t matter: you should never give more than t he bare minimum. Any extra information is unnecessary and could be used against you in the event of a data breach.



Con artists love concerts

Scoring tickets to an upcoming show is exciting but be careful how much you post about it. Scammers can use photos of your concert tickets to create fake ones by copying the barcode. Unsuspecting super-fans then purchase the fakes and steal your seat at the venue. Save yourself the heartache (and the embarrassment) by keeping your concert tickets to yourself.

INFOSEC IQ