The Harm Reduction Approach

Harm reduction is a term used in public health to describe policies aimed at reducing the harm associated with high-risk behaviors, such as intravenous drug use. In the context of digital security training, the harm reduction approach can be applied to populations that are at heightened risk of compromise because of their practices, such as using non-optimal hardware, applications, or platforms. It is not always possible to change an individual's risky practices and when that is the case, it is important to meet people where they are, rather than where we think they should be.

Some principles to follow are:

Everyone deserves digital security and privacy.

It is not uncommon to hear people in the security industry say that if you don't use a certain product or you don't follow a certain best practice, then "you don't deserve security." You may believe that activists should not use Facebook, but if activists still use the platform because it is a highly effective way of reaching their audience, you should give them advice that allows them to be as safe on Facebook as possible.

Remove the stigma of bad security or privacy practices.

Everyone has made digital privacy or security mistakes, including trainers. Stigmatizing or shaming people for confessing their mistakes during a training makes it less likely that other people will speak up about their own practices. Talking about your own digital security shortcomings is sometimes a good ice-breaker and helps make everyone feel more comfortable.

Increasing your digital safety is a process.

When people have recently grasped how much they need to do to improve their digital security and privacy, it's common for them to feel overwhelmed. Encourage people not to be too hard on themselves and to see their work towards better security habits as a process that will take time. No one locks everything down in one day or one week, and it takes a while to learn. As part of harm reduction, it's important to give people props for how they have *already* improved their digital safety as you encourage them to take further steps and solidify better habits.

Harm reduction is collective.

Because of the many ways our digital lives are inherently intertwined, it's important to remind people that we are responsible for each others' safety and privacy. It's upon us to collectively support each other as we learn about each other's privacy preferences. We can coordinate in reducing threats and vulnerabilities that affect us as co-workers, family members, or even just neighbors using the same cafe Wi-Fi to browse the web. When you notice that others have unsafe settings or are leaking personal data, you can tell them. If you prefer not to be tagged in photos on social media, let others know and ask others what their preferences are. If you see your parents have a weak password, take the time to explain how to create a more robust one. There's a million ways we can help our networks reduce the harm from poor digital security habits and build better security cultures.

Si busca la traducción al español de este artículo, haga clic aquí.

For more perspectives on the harm reduction approach as it applies to digital security, check out the following articles.

Just Say No to 'Just Say No' by Mariel Garcia Montes

https://medium.com/berkman-klein-center/just-say-no-to-just-say-no-7726d5cea63c

https://cmsw.mit.edu/mariel-garcia-montes-youth-online-privacy-americas/

Bringing Pleasure Activism to Digital Security and Privacy by Norman Shamas

https://medium.com/@NormanS/bringing-pleasure-activism-to-digital-security-and-privacy-c2fd1b173760

Queer Dating Apps Need to Protect their Users Better by Norman Shamas

https://slate.com/technology/2018/02/queer-dating-apps-need-to-protect-their-users-better.html

Harm Reduction for WhatsApp by Dia Kayyali

https://blog.witness.org/2018/11/harm-reduction-whatsapp/