USERS ARE NOT STUPID:

Six Cybersecurity Pitfalls Overturned

What's the Problem?

The cybersecurity community tends to focus and depend on technology to solve today's cybersecurity problems, often without taking into consideration the human element – the key individual and social factors impacting cybersecurity adoption.

Source: Canva

The Human Element Matters

When organizations fail to consider the human element, there can be real consequences: more calls to the help desk, mistakes that lead to cybersecurity incidents, the use of less-secure workarounds, user frustration, and a perception that security is inconvenient and burdensome.

PITFALLS & MISCONCEPTIONS

1. Assuming users are stupid

Thinking users are stupid or hopeless creates an antagonistic "us vs. them" situation that puts security professionals in a bad light and reduces users' confidence in their own ability to make good cybersecurity decisions.

2. Not tailoring cybersecurity communications

When communicating security information, security professionals may fail to account for differences – like job role and cybersecurity skill level – in their intended audience. They may also have a hard time translating highly technical cybersecurity information into terms that are understandable and relevant to their intended audiences. This may result in people disregarding or misinterpreting important cybersecurity communications.

3. Unintentionally creating insider threats due to poor usability

Unusable cybersecurity systems and processes that require too many steps, too much time, or a technical understanding that many users may not have create undue burden on users. This may result in people making errors, becoming frustrated and anxious, trying less-secure workarounds, or making risky decisions.

4. Having too much security

Users may view overly stringent cybersecurity measures as counterproductive. In addition, the most secure solutions may not be practical or necessary in certain contexts and may have unanticipated consequences for system administrators and end users.

5. Using punitive measures or negative messaging to get users to comply

While use of negative "fear appeals" (scaring users into complying) may have short term behavioral impacts, these may elicit longer term, negative emotions towards cybersecurity. Punishing users when they don't make good cybersecurity decisions – even though they're not experts and struggle with unusable solutions – may further evoke negative perceptions while failing to address the root causes of users' behaviors.

6. Not considering user feedback and user-centric measures of effectiveness

Without collecting concrete evidence of what users are struggling with, it may be difficult to make meaningful improvements to cybersecurity policies, processes, and technologies.

NIST | NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

OVERCOMING THE PITFALLS

1. Empathize and empower.

Thinking users are the weakest link creates an antagonistic "us vs. them" situation that puts security professionals in a bad light and reduces users' confidence in their own ability to make good cybersecurity decisions.

2. Be context aware.

Make an effort to understand your users: their skill levels, roles, constraints, operating environment, and cybersecurity interactions.

3. Be a translator.

When communicating cybersecurity information, use understandable language. Provide context: why it's important and what's expected. Enlist the help of your communications group to craft meaningful messages.

4. Mix it up.

Use a variety of methods and formats to disseminate cybersecurity information to accommodate different user preferences and constraints.

5. Conduct basic usability testing.

Pilot proposed cybersecurity solutions with representative users. Observe errors and ask for feedback. Apply what you learn to improve the solution.

6. Provide actionable guidance and tools.

Present recommended cybersecurity actions in manageable, prioritized chunks easily accomplished by users. Provide tools to help as needed.

7. Offload burden when possible.

Don't expect the impossible or difficult from users when a computer can do it better. Offload user burden to technology when possible.

8. Take a risk-based approach.

Avoid "one-size-fits-all" solutions that may not be appropriate for all contexts. Tailor cybersecurity solutions to the actual risks and capability of your users, including technical and end users.

9. Don't rely on fear alone.

Honestly communicate threats, but don't overstate them. Focus on building users' confidence in their ability to be secure, which can increase their positivity towards cybersecurity and likelihood of taking action. Recognize users that make good security decisions.

10. Gather user-centric data.

Collect indicators of users' cybersecurity attitudes and behaviors, for example, trends in help desk calls or user-level security incidents. Use the data to inform improvements in your cybersecurity program.

You Can Make a Difference

You don't have to be an expert in the human element to make positive changes. Start small by becoming aware of who your users are and how cybersecurity may impact them. Then slowly grow your efforts from there.

Source: Canva

It Takes a Team

Considering the human element ultimately leads to what should be one of your organization's big cybersecurity goals: empowering users of all types to be informed, capable, and active partners in cybersecurity. After all, you can't do this alone!

For more information, visit https://csrc.nist.gov/usable-cybersecurity