Cybersecurity reminders

No one logs in to work for the day thinking, "Today is the day I will be compromised by a cybersecurity attack." And while you may not encounter a cyberthreat this month or even year, it is critical to stay alert to the trends and best practices. This month's newsletter will share a few of the important (but perhaps not so obvious) cybersecurity best practices to keep you and your organization safe this year.

Check email recipients

Sending emails to the wrong people increases the chance of sensitive company or personal information being used by unauthorized individuals.

All information, especially sensitive information, should only be shared with those who need to know. This includes email contents. It is easy to click a recipient that pops up in your email without truly knowing that you clicked the right person. Emails that end up in the wrong hands may be used for malicious purposes.

Investigate hyperlink's destination before clicking

Many times, we encounter websites in the form of hyperlinks. For example, a link that says, "Policy reminders" and takes you to a website or other destination. Hyperlink destinations can be viewed before clicking by hovering over the link with your mouse.

It is important to check the link's destination before clicking. Hackers know that users don't often check links before clicking, and they will hide malicious websites behind hyperlinks. Malicious websites can download malware, scam you or collect your credentials. By checking links, you can avoid these websites.

Review your organizations security policies and procedures

Security policies are put in place to reduce the risk of cybersecurity incidents and increase awareness. In addition to staying up to date with the security policies, reviewing and following all cybersecurity procedures keeps cybersecurity best practices as a foundational part of your workday.

Recent data breach: 23andMe

In October 2023, hackers started selling personal genetic information on the dark web. This information was packaged by ethnic group and appeared to come from 23andMe, a DNA testing service.

23andMe immediately launched an investigation.

What did they learn? The service itself wasn't hacked. Instead, attackers used a technique called "credential stuffing." They took login information and passwords stolen from other services – such as email programs and online shopping platforms. Then they tested these logins and passwords on 23andMe.

Unfortunately, many people reuse login and password information across different sites. And some of these stolen credentials allowed hackers to log into real 23andMe accounts.

UMass Boston

Have you been breached?

Data breaches are happening every minute. With so much of our lives online, there is a high chance that our emails, usernames and passwords have been seen by an unauthorized user. Troy Hunt created the Have I Been Pwned site with public service in mind. He wanted to not only support the public in protecting their data, but also inform people how rampant and serious data breaches are. If you are interested, head over to https://haveibeenpwned.com to see if you have been impacted by a data breach.

More about HIBP can be found on their FAQ page.
https://haveibeenpwned.com/FAQs