

SecurityAwarenessNews

the security awareness newsletter for security aware people



Cybercrime & You



How Data Breaches Happen

The Personal Impact of Cybercrime

The Threat in Your Pocket

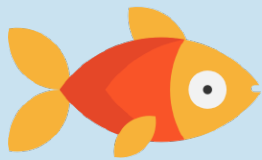


How Data Breaches Happen



Equifax, Yahoo!, Uber. Just a few household names who have suffered massive data breaches, which affected billions of people worldwide. But how?

Spear Phishing



Spear phishing targets specific people at specific organizations. Such was the case for Yahoo!, whose data breach was *made possible by someone clicking on a spear phishing link* that ultimately provided access to a massive database of user information.

Source:
[CSA Online Article - Inside the Russian Hack of Yahoo and How They Did It](#)

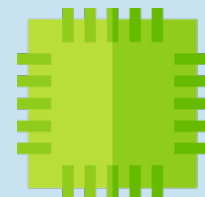
Stolen Credentials



One breach leads to another! When millions of login credentials get exposed, attackers try to use those credentials to access other accounts. In the case of Uber, the *attackers leveraged a stolen username and password* and successfully logged into Uber's database of private user information stored on an Amazon server.

Source:
[CNN Money Article - Uber's Massive Hack, What We Know](#)

Unpatched Vulnerabilities



Cybercriminals don't always kick down the front door (login credentials); sometimes, they'll see if the backdoor is unlocked. Equifax learned this the hard way when they *failed to update a device* that scans for malicious activity.

Source:
[ZD Net - US Government Releases Post-Mortem Report on Equifax Hack](#)



Human Error

Human error is the root cause of almost every breach. Clicking on a phishing link. Using weak passwords. Failing to update software and firmware. Accidentally uploading sensitive data to a public forum. None of these require "hacking," and they're evident in every example above.

Regardless of how data breaches happen, they impact all of us. On a professional level, our organization stands to incur extensive damage with long-lasting effects. On a personal level, few things are worse than having our highly sensitive information end up in the hands of criminals. Help prevent that from happening by staying alert, remaining skeptical, reporting security incidents, and always following policy!



The Personal Impact of Cybercrime

When an organization suffers a data breach, the net results can cost millions, while permanently damaging relationships with our clients and customers. That's a big part of why we take our security policies and awareness training so seriously.

But we take the *personal impact* of data breaches just as seriously, because at the end of the day, we are all subject to having our personal data compromised. Here are a few examples of cybercrime that impact each of us on a personal level, and what you can do to prevent it.



Identity Theft

Perhaps the most immediate threat in all cases, identity theft allows cybercriminals to open accounts, make purchases, or even file tax returns in your name, among other things. **One way to avoid this is to limit the amount of personal data you make public.**

Also, know that government entities won't email you asking for payments or sensitive info. Consider placing fraud alerts or freezes on your credit reports.



Phishing

Cybercriminals use phishing attacks to execute a wide range of malicious intentions, from stealing data to obstructing operations. Stay alert for any messages that contain awkward or poor grammar, threatening language, or random links. **Remain highly skeptical of any requests for sensitive info.**



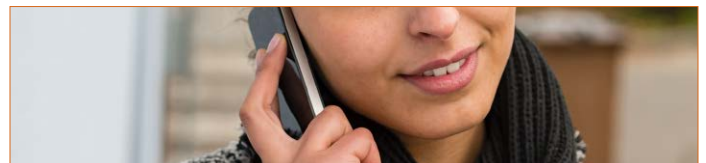
Ransomware

A form of malware that encrypts files and systems until a ransom has been paid, ransomware yields scary results, such as when hospitals are unable to access databases or cities are unable to render public services. But criminals will happily target individuals, as well. Don't fall victim. **Think before you click**, and never download random attachments in emails.



DDoS Attacks

Short for distributed denial-of-service, criminals use DDoS attacks to shut down websites and knock all internet services offline, usually impacting millions of people. DDoS is made possible by smart devices left unprotected. That's why it's imperative that you **update default usernames and passwords of connected devices** ASAP, and enable auto-update of apps and smart devices wherever possible.



Vishing

Short for voice phishing, vishing attackers utilize telephone services to trick victims into divulging financial or other forms of private data. Just like with phishing, we need to treat random requests for data with a high degree of skepticism. **Never assume someone is who they say they are**, and don't blindly trust a caller ID, since cybercriminals figured out how to spoof those years ago.

Remember, preventing cybercrime starts with common sense and ends with following our organization's policies. If you ever have questions about our security efforts, please don't hesitate to ask.

The Threat in Your Pocket



Why do cybercriminals target smartphones?

The obvious answer: there are a lot of them. Estimates show that over 5.1 billion people own a smartphone. That's a massive target oozing with hacking potential.

Source: [BankMyCell.com Blog - How Many Phones Are In The World?](#)

What makes mobile devices so vulnerable?

Smartphones have screen-size limitations that restrict what can be viewed. For example, it's difficult to hover over links to show their full URL or to ensure that a webpage is legitimate. Also, people are easily distracted when using smartphones and will often click quickly, without much thought.







How common are mobile attacks?

App stores struggle to catch malicious developers due to the sheer number of new apps uploaded every day. Not long ago, a research company identified six malicious applications which already had over 90 million downloads. Furthermore, cybercriminals utilize text messaging to send malicious links while impersonating financial institutions, charities, government agencies, utility companies, etc. Mobile devices have quickly become one of the top attack vectors for cybercriminals.

Source: [Checkpoint Research Article - PreAMo: A Clicker Campaign found on Google Play](#)

What can we do to prevent mobile cybercrime?

First and foremost, treat your smart device like a computer, which is what it is. That means you need to be:

-  Utilizing antivirus software and enabling automatic updates.
-  Staying alert for phishing attacks, which come via email and texting on smartphones.
-  Never connecting to public WiFi without a VPN—a virtual private network that encrypts your connection.
-  Vetting all apps before downloading AND regularly removing unused apps.
-  Allowing only the minimum number of permissions needed for an app to properly function.
-  Always following our organization's mobile device policies.