Cyber Security Awareness Newsletter

Protecting yourself and information from cyber security threats

As we begin 2022, we wanted to bring your attention to 6 cyber security myths/misconceptions that prevent folks from being properly secured and protected.

Myth #1 My Anti-virus software is the only thing I need to protect my machine.

Anti-virus software searches for specific types of viruses/malware and stops the actions based on behavior/file type names, and has some phishing protection and protections against malicious websites. Not all actions on a system are seen as malicious by a virus scanner, however, and you should implement other provisions to help secure and protect your system. Please visit our website https://security.bsd.uchicago.edu/ for further information on protection and security for your system.

Myth #2 We aren’t important enough for criminals to want our data.

Every user with an account at the institution is important. It doesn’t matter if the account has admin rights or not. Any account can be weaponized to create malicious activity or gather further information that can be used for further malicious activity. The goal for all cyber criminals is to exploit the chain of command, which is almost always known in any organization, and ultimately gain access and control to valuable assets.
Myth #3 Cybersecurity threats are only external.

Insider threats are very real. One of the most overlooked internal threats stems from the human component. An accidental or purposeful click on a malicious e-mail or other socially engineered threat (accidental loss or disclosure) that compromises a machine isn’t the only threat we face internally. Use of third-party unapproved software (Shadow IT) or use of unauthorized devices can become a legal liability. There is no denying that some unapproved tools (like USB drives) are convenient to use, but they must follow security policy standards. Unapproved software also requires a security review before implementation. Employee sabotage, theft of data, unauthorized use/access, or following weak and unsafe practices can all stem from stressors, and/or behavior with malicious intent.

Myth #4 3rd party security providers take care of security needs.

Not everyone’s data is sensitive and not everyone’s needs are the same. Third party providers such as application or cloud-based vendors won’t meet your security needs unless you explicitly ask them, and they are capable of providing the service. In 2020, Amazon, eBay, Shopify, and Paypal all fell victim to a massive data leak due to a 3rd party UK security provider who handled their database. In 2020, GE
reported another data breach caused by their service provider, Canon Business Process Services, who leaked personally identifiable information of GE’s beneficiaries and employees, both current and former.

Myth #5 Once we have achieved complete security compliance and our security strategies are in place, we have met our security needs.

Cyber security complacency is a common catalyst for cyber security breaches. Complacency can reflect overconfidence when it comes to pursuing higher standards or stronger achievements. In an ever-evolving security threat landscape, things like overconfidence, “good enough” security mentality, sticking with what we know, and reluctance to let go of outdated processes, solutions, and technologies give threat actors opportunities to respond. Cybersecurity threats emerge often, and complacency is not an option in cybersecurity. Continuously updating technology, becoming familiar with the latest criminal activities and how to mitigate and discover them is a fact of continuous necessity.
Myth #6 Too much security diminishes productivity

When properly vetted and properly implemented, security controls become a seamless part of day-to-day work. A correct balance between protection and productivity must be found for all aspects of work. Doing away with security controls can have severe and, in some cases, catastrophic legal consequences. A successful attack on one employee can ripple through the entire organization causing business to come to a standstill. Recovery of a breach may take days and sometimes even weeks in loss of productivity. A modern cybersecurity approach uses security tools that are seamless in practice and help detect and mitigate threats while also leveraging productivity.

<table>
<thead>
<tr>
<th>Prevents attacks</th>
<th>Limits extent of attacks</th>
<th>Recovers data &amp; system availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Whitelisting</td>
<td>Restrict Admin Privileges</td>
<td>Daily Backups</td>
</tr>
<tr>
<td>Patch Applications</td>
<td>Patch Operating System</td>
<td></td>
</tr>
<tr>
<td>Configure Microsoft Office Macros</td>
<td>Multi-Factor Authentication</td>
<td></td>
</tr>
<tr>
<td>User Application Hardening</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>