Empowering Educators: Cyber Acuity with Security for 21st Century Classrooms
ACODE 89 Workshop 13/14 July 2023

Hosted by Griffith University

Executive Summary

"Data is the new oil...don't let it slip!"

The ACODE 89 workshop was held on Thursday 13 July 2023 in partnership with CAUDIT on the topic of empowering educations: cyber acuity with security for 21st Century Classrooms. Just over 40 attendees represented a broad range of roles from across the L&T sector, including teaching academic staff, educational designers and technologists, directors of learning and teaching, and learning support specialist staff.

Key points shared during the workshop

- Cybersecurity is a shared responsibility across organisational levels
- Individuals can take simple steps to protect themselves and the data they have access to. Institutions have a role to play to develop the digital literacy and fluency of staff and students.
- Polite cautiousness or being professionally paranoid about unexpected emails, phone calls and texts are useful techniques to minimise cyber threats and risks.
- Acuity is a core life skill that helps produce smarter graduates and employees.

Keynote

Thomas King, Higher Education Industry Executive, Microsoft ANZ

"We need to get it right every day. Hackers only need to get it right once!"

Cyber security can seem endlessly complex with many moving parts such as devices we use to access resources and connect with each other, and devices that power our campus infrastructure. Many of our teaching and learning technologies are delivered software as a service (SaaS) yet require integration across systems. Further complexity occurs in hybrid infrastructures, identity and access management across many different technologies. Consider these components like moving puzzle pieces with thousands of threats looking for vulnerabilities.

While cyber professions have frameworks and technologies to manage the complexity of secure university, individuals have a significant role to play. Thomas shared four key things we can do to protect and manage our data. These recommendations are:

1. You and your digital identity are valuable. **Multi-factor authentication (MFA) and strong passwords** are protective shields in your cyber protection efforts.

2. Make sure the **devices you use are secure** and keep your software up to date, automatically as much as possible.

3. Ensure you have **least privilege rights**, or in other words only access the data you need to do your job.

4. Think about your contribution to **reduction of software sprawl** at your institution by proof of concepts, pilots of new technologies, and the applications you must use to do your job to ensure competency and security/infrastructure approval status. Become experts in the applications you use as there is a direct correlation between identifying phishing attempts and competency in the applications.

Cybersecurity 101: Defending our Digital Environments and Empowering Educators
Nikki Peever, Director Cybersecurity (CAUDIT)
Jakob Sellmann, Cybersecurity Officer (CAUDIT)

"Criminals collaborate...we need to copy the criminals to improve our defences together"

Understanding the behaviours of cybercriminals is key to defending our digital environments and empowering educators. Common techniques used by cybercriminals include deceptive calls, texts and emails that mimic something or someone you know and coercing you to act urgently. To combat these techniques **be politely cautious,** pause and assess what the action request is and whether it is a legitimate request. Cybercriminals seek to create a situation of fear, curiosity, urgency, and intimidation (social engineering), and it is okay to be professionally paranoid and politely cautious about every email, text and call you receive.

Universities may be seen as a soft-targets due to the complexity of systems in place and the valuable data they collect, store and use. For instance, information on students (past, present, potential), staff (past, present), research participants and research data, financial data, and IP. However, not all threats are externally generated and may be internal through accidental or malicious actions. Defending yourself from cyberthreats is simpler than you think, and four strategies were shared.

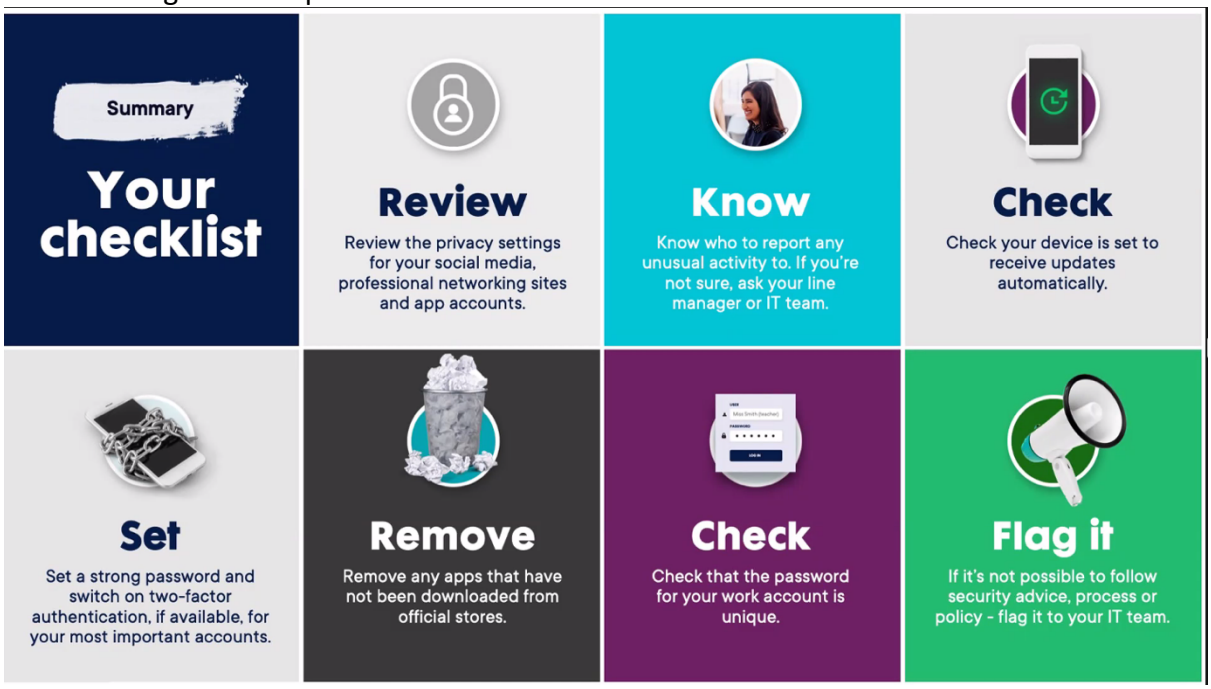
1. Defend yourself against phishing attempts – be politely cautious.

2. Use strong passwords with multi-factor authentication. The longer the password the stronger it becomes, such as three random words with special characters added in. Store passwords securely and use a separate password for work accounts.

3. Secure your devices by applying software updates as soon as they are released and physically protect your device.

4. If in doubt, call it out by reporting any suspicious activity as soon as possible, and don't be afraid to challenge the level of security in place at your work instead of taking workarounds.

The following checklist provides a useful overview:



Sector Roundtable – What's happening around Cybersecurity at your Organisation

Training: cyber essentials training modules and responsible data use resources to help staff and students create strong passwords and manage their information securely. Training modules are contextually situated to help make the activities relevant to different roles. Mandatory training is common however, voluntary take-up of resources or smaller just-in time, bite-sized, modules tend to be low.

Engagement: Some organisations are using mechanisms such as Communities of Practice, working parties and 'cyber champions' to help 'spread' acuity and identify collaboration opportunities across areas outside of traditional IT departments.

Software and system: Examples shared included emails flagged as [External] with cautionary notes applied, in-context reporting and blocked emails requiring vetoing to view. Some institutions send cyber-security equivalent of a fire drill with emails designed to test system vulnerabilities and user-behaviour with phishing emails. Multi-factor authentication for staff is a common approach broadly applied across university systems; however, MFA was not widely applied for students' access to all university systems or infrastructure. Assessing and managing tech-debt is an emerging approach as institutions manage the software and system sprawl across the enterprise.

Governance: appointments of Chief Information Security Officers, or Chief Security Officers are providing executive level stewardship across university systems and data.

Strategies for promoting cyber acuity in students within the 21st Century Classroom

Cybersecurity is 'everyone's business' and is more than phishing attacks on email. There are associated rules and policies supporting cybersecurity approaches, however promoting acuity leads to smarter graduates and employees.

For students, cybersecurity is a core life skill as students develop their abilities to manage and protect their personal cybersecurity, personal privacy, and identity. Further dimensions are layered on top of these skills in discipline practices such as workplace security and client confidentiality. Strategies shared include the following:

In class:

- Including cybersecurity practices and techniques in activities like case studies, simulations, guest speakers, and interactive workshops.
- Academics leading the way by showing their cybersecurity practices such as not using USBs or leaving open laptops in computer labs.
- Signage in teaching spaces about laws, policy and advice around recordings and broadcasting video during hybrid classes.
- Promoting cybersecurity practices at orientation activities as students start their university journey.

In curriculum:

- Learning materials and activities that promote the handling and maintaining confidentially of data relevant to the discipline and profession.
- Develop students' digital literacy and fluency in discovering, evaluating, and using information effectively and ethically.
- Embed cybersecurity techniques in graduate attributes so it is embedded across their program of study.

Online:

- Training modules, and resources on cybersecurity, privacy, and data handling agreements for the educational technologies they use at the university.

In assessment:

- Embedding digital citizenship skills in assessment tasks to enable them to participate in online communities safely, ethically, and respectfully.

Supporting our Teaching Teams: Where cybersecurity meets curriculum and how we support it

For teaching teams, institution-wide strategies are required to support them in developing their own digital fluency and literacy skills and enable them to embed cybersecurity practices and techniques into the curriculum. Mandatory training is common but underutilised and resisted. Usability and security of technology are seen as opposing forces and finding the 'sweet spot' is a challenge and strategies to address this challenge shared

included ‘coffee vouchers’ for engaging in non-common features of enterprise software and providing easy ways to access supported and approved tools.

Attendees shared some of the barriers facing teaching teams such as a lack of authentic connection between IT departments and teaching teams which result in resistance to applying cybersecurity techniques in their practice or completing training modules.

Strategies for supporting academic staff:

- Identifying who takes responsibility for cybersecurity acuity across centralised departments and how they will partner
- Providing explicit listings of approved and supported virtual learning environment (VLE) components (educational technologies). In parallel, listings of technologies that have not been approved in line with the rationales/considerations for non-implementation.
- Ensuring professional development for academics in the use of educational technologies has embedded components of cybersecurity enhancing the acuity and active engagement with linkages between tech and activity/assessment design.
- Working collaboratively with other areas to determine linkages for support and provide risk mitigation across educational use-cases.
- Implementing awareness and/or incentive programs. Coffee vouchers are very attractive.
- Making explicit linkages between ‘enterprise’ modules for staff/students and strategies for embedding continued awareness and practice in courses.

Barriers & considerations:

- VLE Management at Enterprise level – finding the ‘sweet spot’ between usability vs security
- Decentralisation of system management, collaborative mechanisms should be put in place
- Academic/staff time and limited ability to incorporate more content in the curriculum.
- Getting buy in across specific departments – targeted awareness based on use-cases should be garnered to support engagement
- Size, complexity & turnover across Institutions – acuity must be embedded in practice

Other affordances & enablers:

- Implementing industry access to supporting tools (eg. VPN Labs, Cyber ranges)
- Leveraging In-context support mechanisms embedded within systems for example Pop up messages on ‘creation of online assignment’, reminders etc.

Generative AI in Australian Higher Education (July update)
Michael Sankey, ACODE President

A whitepaper from ACODE will be forthcoming about Generative AI in Australian Higher Education. Thirty-eight responses were received to a recent Generative AI survey representing 34 institutions.

Survey highlights include:

- Changes to assessment practices are starting to emerge with examples shared in the survey responses.
- Updates to policies and procedures are occurring across the sector, accompanying the provision of centralised workshops and resources to support staff and students in ethically and effectively use Generative AI.
- There is a progressive shift being seen across the sector in encouraging students to use Generative AI in their work but analyse, improve, and reflect on their work.
- There is a trend observed in how exams are managed across the sector.

Further insights into Generative AI in the sector can be found in the whitepaper when it is available. No spoilers here!