8. Cybersecurity on a College Campus

Goodman College, a small undergraduate liberal arts school with enrollment of about 3,000 students, struggled through the last two decades without a director of information services. It managed as best it could with limited resources and limited expertise. Recently, during a round of accreditation review, auditors criticized the college for having a weak password policy that did not provide adequate protection for information stored in the university’s systems. According to the old policy, passwords had to have exactly eight characters, and could be anything printable, including dictionary words or repeated characters. Passwords never had to be changed, and the system would not keep someone from guessing repeatedly at passwords.

On numerous occasions, student and faculty accounts were compromised, although it always turned out to be due to someone running an infected email attachment; there is in fact no evidence that anyone’s password had ever been cracked. Nevertheless, the information technology team, in responding to the auditors’ criticisms, implemented a much stricter password policy. Passwords had to be changed every 90 days. No password could ever be reused. Every password must contain at least one lowercase letter, at least one uppercase letter, at least one number, at least one other character excluding “@,” no words or phrases found in English or foreign dictionaries, and it must be at least 10 characters long. Furthermore, once accepted, a new password could not be changed again for 30 days. After three failed attempts at guessing a password, the account would be locked until the user showed up in person at the help desk with a valid school ID and requested a password reset. The help desk is open from 9:00am till 4:00pm Monday through Friday on schooldays and closed other days.

The new policy satisfied the auditors but infuriated both faculty and students. Faculty complained that they have used their favorite passwords at other online services for over a decade without ever having to change. They said that having to change passwords so often and having to jump through so many hoops would dramatically increase the likelihood of forgetting their passwords. They said that getting locked out of their accounts and being forced to wait for the help desk’s business hours could be a disaster on weekends, holidays, or at night, the very times when they would normally be doing much of their online work. They further predicted that the same problems the faculty experienced would also plague students, who could be locked out of assignments, projects, tests, email, and so forth.

The members of the password policy committee listened politely to faculty complaints and pointed out that they had no choice in the matter. The auditors had spoken, and that was that: They had condemned Goodman’s previous password policy, demanding that it more closely conform to “best industry practices.” Faculty appeals based on the unreasonableness of the new policy, or the personal hardship it would cause, or the predictable interference with the educational goals of the university fell on deaf ears.

In an effort to placate some particularly vocal faculty members, the chair of the password policy committee explained that a compromised email account from the “.edu” domain (like Goodman’s) is especially dangerous. Accounts ending in “.edu” are not as carefully filtered by major providers, and when such accounts start spewing out SPAM, the entire university gets blacklisted by many companies. It takes many hours to get the university’s name removed from
blacklists. “Keeping all our users’ accounts secure is not only our duty to the individual user, but to the rest of the school, and to the academic community as a whole.”

Shortly after this conversation, the chair of the password policy committee noted to one of the faculty members that another (anonymous) faculty member’s account had become compromised on Friday, and the understaffed and overworked technology team had spent about twenty extra hours on the weekend getting Goodman off of several blacklists. The incident, while illustrating the dangers of compromised accounts, had not actually come from a cracked password.

Soon, faculty and students alike began keeping written and electronic records of their latest passwords in easy-to-find locations. Predictably, after many years of not having any passwords cracked, these new insecure methods started to produce a trickle of compromised accounts.

Seeking a quicker response from the administration, one small group of students began a protest movement. Every Friday afternoon and every day before a holiday, the members would go off campus and anonymously attempt logging in multiple times to the accounts of every administrator, effectively locking the entire administration out until the help desk reopened.

Case from the 2016 Intercollegiate Ethics Bowl National Competition
© 2016 by Robert Boyd Skipper, Peggy Connolly, Ruth Ann Althaus, Heidi Malm