NYSED Privacy Office Newsletter
Volume 1, Issue 3
April 2022

A Message from our CPO:

Happy Spring to all of our DPOs! As NYSED's privacy office continues its outreach and introductions to the State's educational agencies and DPOs—which includes these newsletters—you will see that we often cite back to the findings in our Annual Report. The 2021 report found that human error was the underlying cause of just about half of the reported data incidents. However, many articles on cybersecurity and data privacy say that 95% of cybersecurity breaches are caused by human error.

What to do with statistics like that? As we say in the Privacy Office: when your problem becomes my problem—it's a problem. The first step is to assess your organization's cybersecurity awareness. Be honest and realistic about what your staff knows and doesn't know. Once you know the scope of your "problem" you can plan accordingly—by reinvigorating your training or placing increased controls on your school's data, among other actions. Although we sometimes want to look away, understanding the scope of the problem is the first step toward correction and ultimately better data security.

~Louise DeCandia

Preventing unauthorized disclosures of Student PII and APPR Data

As we strive to effectively communicate with students, staff, and parents, we need to safely navigate through the intersection of Communication and Privacy to avoid accidental unauthorized disclosure of protected Student Data and APPR Data. While an automobile can be fixed at a repair shop, it is more difficult to fix an unauthorized disclosure of protected data.

In 2021, our office received more reports of inadvertent unauthorized disclosures than it did in 2020. Many of these unauthorized disclosures could have been avoided.

QRishing – A threat on the rise

During COVID, these little square 3d code boxes popped up everywhere from restaurant menus to product boxes at retail stores with the promise that one could enjoy contactless transactions just by scanning the square. These square boxes are Quick Response Codes, or "QR codes." While you may not have noticed QR codes before COVID, they have existed since 1994.

QR codes are a convenient way to transact business; however, they also pose a significant security threat to your mobile device because once the QR code is scanned, the code embedded in the QR code automatically executes. QR Codes are easy to generate. Due to their design, it is difficult to determine whether a QR Code is a fake.

Other than not scanning QR codes, what can you do to protect yourself and your school against QRishing?

- Add an antivirus/anti-malware application to your and school issued mobile devices.
- Check the Uniform Resource Location (URL) before allowing a QR Code to open a browser to mitigate the risk of malware or other adverse consequences.
- Train staff to be aware of the hazards of QR codes.

To read more, visit https://www.forbes.com/sites/louiscolumbus/2020/09/20/the-cybersecurity-threat-no-one-talks-about-is-asimple-code/?sh=796dff327e2a

How many 2-d terms can you find?

There are 18 terms. The list and solution are below

D	A	T	E	N	C	R	Y	P	T	I	O	N	E
D	I	S	I	I	H	A	P	E	T	C	O	N	P
D	S	S	H	P	T	I	T	O	P	D	F	D	A
N	T	O	T	O	O	I	R	T	L	P	Y	R	R
E	I	I	Y	C	A	V	I	R	P	I	C	E	E
I	P	Y	B	R	E	A	C	H	C	T	C	T	N
S	T	U	D	E	N	T	D	A	T	A	T	Y	T
P	A	T	N	O	T	I	F	Y	C	C	A	N	S
T	R	R	C	O	M	P	L	A	I	N	T	S	Y
E	R	U	S	O	L	C	S	I	D	I	O	T	D
Y	R	O	T	C	A	R	T	N	O	C	O	S	P
N	L	I	F	P	P	C	P	I	I	C	T	R	A
E	G	S	I	T	C	E	T	O	R	P	T	Y	O
D	C	T	F	R	I	G	H	T	S	O	C	M	Y

Tips for avoiding an unauthorized disclosure

- Require onboard training. Before providing a new employee with access to Student PII or APPR Data ("protected data"), provide the new employee with training on Education Law § 2-d and FERPA rules regarding disclosure of protected data and make sure that the new employee understands the rules.
- For the school and school district remote devices, such as laptops, Chromebooks, and tablets, review the installed applications to determine whether they are necessary. Remove any unnecessary applications.

- For all school and school district devices that might be connected to your network, do not allow the installation of platforms or applications without consent from the technology department.
    - In Windows 7, 8, 10, and 11, as well as the Windows Server family, you can restrict users from installing new programs using the Group Policy Settings. These settings provide an option to restrict the installation of new programs to only those offered by the technology department.
    - For Google, application management is available through the Google Admin console. Information regarding application management and disallowing installation of unapproved applications can be found at: https://support.google.com/a/answer/6089179?hl=en
    - For Apple products, including Macs and iPads, Apple provides support for education users at: https://support.apple.com/education. Apple's support includes a deployment guide, which can be found at: https://support.apple.com/guide/deployment-education/welcome/web.
- Ensure that all school and school district devices are encrypted, regardless of whether a device can be connected to your network. Remember that student names and other identifying information that can be used to log into resources may be stored in a browser's cache and need to be protected from unauthorized disclosures.
- Disable the ability for any browser or application to store a user's name and password.

Wordsearch Terms: Student Data–Contractor–DPO–Policy–Breach-CSF-Complaints-DPA-Notify-NIST-Privacy-Disclosure-PII-Rights-Encryption-Parents-Protect