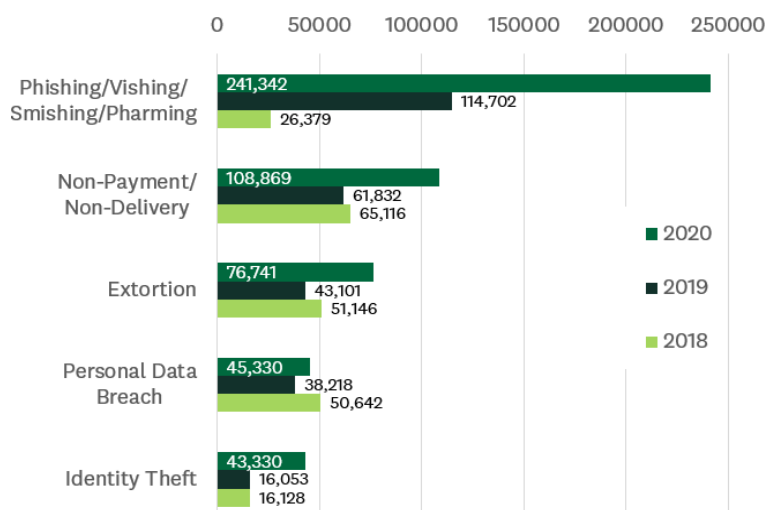


Finance & Admin Update

Announcements and updates from Finance, Campus Services, Human Resources, and Risk & Internal Controls

Chart of the Month

Cybersecurity Month: Cybercrime Incidents in 2020



Source: [IC3 2020 Annual Report](#)

The COVID-19 global pandemic presented a significantly increased opportunity for criminals to target individuals that isolated at home and used the internet for online shopping, social media, news, and other sources of entertainment. In the [Internet Crime Complaint Center \(IC3\) 2020 Annual Report](#), FBI data shows a significant increase in fraud complaints, more than doubling in Phishing, Vishing, Smishing, Pharming in attempt to gain access to Personal Identifiable Information (PII), leading to extortion, identity theft, and ultimately financial loss. Check out page 2 for more information on “Phishing, Vishing, Smishing, and Pharming”.

Non-Payment/Non-Delivery is another area that had a significant increase over the past year. Non-payment/non-delivery occurs when either items that are received are substantially different or completely different from what was ordered, or no order is received at all

To protect yourself from scammers:

- ✓ Always use extreme caution in online communication
- ✓ Verifying the sender
- ✓ Hover your mouse over a link before clicking to see where it is sending you.
- ✓ If a deal is “too good to be true”, it probably is.
- ✓ Use trusted sources, when verifying information, shopping, and browsing.

Check out Finance’s [Cybersecurity & Fraud Prevention](#) site for more informational resources and training.

2022 Open Enrollment Starts Today

The calendar 2022 Benefits Open Enrollment period for faculty and staff began today, Monday, October 18th at 8:00AM and will close Monday, November 1st at 11:59PM. This is your annual opportunity to review and change your benefits for the next calendar year.

Go to dartgo.org/benefits2022 to sign up for live events, view prerecorded information on benefit changes, get one-on-one assistance, and access important information.

Live 2022 Benefit Webinars are available:

- Tuesday, October 19 from 10:00 – 11:30AM
- Thursday, October 21 from 2:00 – 3:30PM

Additional Personal Day

President Hanlon announced that each employee will be provided an additional Personal Day. For benefited employees, these hours are available effective October 5. The additional personal day was included in the balances in Kronos for hourly employees on Thursday, October 14th and was reflected on the Friday, October 15 payslip. This additional personal day should be recorded as a normal personal time, using the “Per” pay code in Kronos.

Check out the [Additional Personal Day FAQ](#) for more information.

Employee Bonus and Increases for Student Minimum Wage and Financial Aid

On October 11, 2021, Dartmouth [announced](#) increased financial aid to undergraduate students and several wage-related initiatives for faculty, staff and student employees. Please reference the FAQs now available online:

- [Employee Bonus FAQs](#)
- [Student minimum wage increase FAQs](#)

Returning Funds for Personal Expenses

Dartmouth employees now can return funds for personal expenses charged to either a Dartmouth corporate card or procurement card (PCard) via personal credit or debit card.

When returning funds on a corporate card, you will need to know the amount due and the OIE number of the Expense Report that the personal expense was reported on. When returning funds for PCard charges, you will need to know the amount, chart string, and the OB number of the PCard eForm used to report the personal expense.

For more information and to access the payment portal go to [Returning Funds for Personal Expenses](#).

Phishing, Smishing, Vishing, Pharming

Phishing, the most used method, is fraudulent emails attempting to respond either by click on that takes you to a fraudulent site or downloads malware or ransomware on your device. But many may not be aware of other methods.

Vishing, Smishing, and Pharming are less well known.

- **Vishing** is voice phishing.
- **Smishing** is SMS (short message service - often referred to as messaging, texting, or chat) phishing.
- **Pharming** uses the DNS cache on the end user's device or on a provider's network equipment and usually is used to obtain personal or banking information.

Contracting: Clickwrap Agreements

Clickwrap agreements, also known as a clickthrough agreement and clickwrap [license](#), are a form of agreement used for [software](#) licensing, websites, and other electronic media. Clickwrap agreements requires the user to agree to terms and conditions before using a website, completing an installation or online purchase process. These agreements typically present the terms and conditions followed by a check box with the words "I agree" or "I accept" that the user must click.

Some examples of transactions that would require the user's assent to a clickwrap agreement are:

- Downloading or installing software.
- Purchasing an airline ticket or online music.
- Registering an account on a [social media](#) website.
- Using a website.

When purchasing or registering online, you may be agreeing to Vendor's terms. Under Dartmouth purchasing policies, vendor contracts should be reviewed by [Procurement](#) to ensure that they do not present unreasonable risk to the institution. This is especially important where the product or services involved present exposure for the institution, like software that involves sensitive Dartmouth data, or services that involve a vendor having access to sensitive populations.

Time to Transition off Internet Explorer

Microsoft is no longer supporting Internet Explorer 11 for use with Microsoft 365 apps and services (including browser versions of Outlook, Word, Excel, etc.). ITC recommends that users move to fully supported browser versions of Edge, Safari, Chrome, and/or Firefox. For resources to help with the transition go to:

[Set Default Web Browser](#)

[How to move Browser Bookmarks](#)

[How to access your Internet Options without IE](#)

If you are using Firefox to access java modules in Oracle, such as PCard Transaction Maintenance, ITC recommends that you [download the Firefox ESR version](#).

PaymentWorks Vendor Portal Reminder

Dartmouth College has partnered with PaymentWorks to handle the collection, validation, and management of all vendor information. It is important to encourage vendors to register within the PaymentWorks Vendor Portal to help prevent fraud and provide payment protection. This system allows for vendors to easily manage their profile, contact information, preferred payment method, and view the status of their payments and payment history. The portal also allows the vendor to provide important tax, insurance, and various certificates without having to send this information through email.

Encourage your vendors to visit the [Vendor Guide](#) and review the [PaymentWorks Vendor Portal](#) information if they have questions. If they need additional support, please have them visit the [PaymentWorks for Payees](#) site and click the [Support Center](#) at the bottom of the page.

For more information check out the [PaymentWorks FAQ for Departments](#).

PCI DSS Training

If you participate in the acceptance of credit card payments and have access to the files, system, or service that retains sensitive cardholder data in paper or electronic format, you should have received an email invitation to participate in PCI DSS training (Payment Card Industry Data Security Standard).

This is an online training module that has been selected by the Information Security Group to help Dartmouth keep staff in compliance with PCI Data Security Standards. Please allow approximately 30 minutes to complete the training. For more information regarding PCI compliance, you can go to this URL: <https://www.pcicomplianceguide.org/faq/>

Records Management

All records produced and maintained by employees of Dartmouth College remain the property of Dartmouth, and should not be removed, altered, or destroyed, except as provided within Dartmouth's record retention policies.

Records Management is responsible for educating and guiding Dartmouth personnel as they make decisions regarding the proper production, maintenance, and long-term use of their recorded information. More information is available at the following resources:

[Records Management and Archives Access Policy](#)

[Records Retention and Destruction Policy](#)

[Records Management Quick Review](#)

[Records Management Training Resources](#)

For assistance in determining if you have records of continuing value to Dartmouth that need to be managed, contact [Records Management](#).