

Stalkers using computer cam recorders

Stalkers have been known to get information from home computers through the computers' cam recorder. They hack into the computer and can see / record images through the cam recorder on your computer. They can see if someone is home and watch them through the camera. Note – computer does not have to be turned on; and you do not have to give them access. This is particularly disturbing with computers in bedrooms.

You can stop this by covering up the camera with a piece of black tape. Or power off the computer **AND close the lid**.

Phishing Attacks – Financial Fraud

Phishing is a type of attack whose goal is to steal private information, such as login credentials or credit card numbers, usually to carry out various types of financial fraud. An attacker impersonates a trusted entity, such as a bank, government, or large web site, and tries to trick people into giving up their private information. These attacks often take the form of "urgent" emails asking people to take immediate action in order to prevent some impending disaster.

Examples include topics such as the following:

"Our bank has a new security system. Update your information now or you won't be able to access your account."

"We couldn't verify your information; click here to update your account."

Sometimes the email claims that something awful will happen to the sender (or a third party), as in "The sum of \$30,000,000 is going to go to the Government unless you help me transfer it to your bank account."

People who click on the links in these emails may be taken to a phishing site - a web page that looks like a legitimate site they've visited before, but is actually controlled by an attacker. Because the page looks familiar, people visiting these phishing sites enter their username, password, or other private information on the site. What they've unknowingly done is given a third party all the information needed to hijack their account, steal their money, or open up new lines of credit in their name. They just fell for a phishing attack.

The concept behind such an attack is simple: Someone masquerades as someone else in an effort to deceive people into sharing personal or other sensitive information with them. Phishers can masquerade as just about anyone, including banks, email and application providers, online merchants, online payment services, and even governments. And while some of these attacks are crude and easy to spot, many of them are sophisticated and well

constructed. That fake email from "your bank" can look very real; the bogus "login page" you're redirected to can seem completely legitimate.

These tips are brought to you by [Olds-Didsbury-Sundre Rural Crime Watch](#). Check out our website for more information and how you can join and get involved with crime prevention. Everyone is welcome. Whether a rural or municipal resident, or business, you are welcome to join us. Membership forms and meeting dates are on our website.
